ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ ИНСТИТУТ
МЕЖДУНАРОДНЫХ ОТНОШЕНИЙ (УНИВЕРСИТЕТ)
МИНИСТЕРСТВА ИНОСТРАННЫХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ»

На правах рукописи

Цыплакова Алёна Дмитриевна

ПРОТИВОДЕЙСТВИЕ КИБЕРПРЕСТУПЛЕНИЯМ В ОТДЕЛЬНЫХ СТРАНАХ ГЛОБАЛЬНОГО ЮГА

Специальность 5.1.4. Уголовно-правовые науки

Диссертация на соискание учёной степени
кандидата юридических наук

Научный руководитель:
доктор юридических наук, профессор,
Заслуженный юрист
Российской Федерации
Волеводз Александр Григорьевич

Москва – 2025

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ 5

ГЛАВА I. УГОЛОВНО-ПРАВОВОЕ СОДЕРЖАНИЕ КИБЕРПРЕСТУПЛЕНИЙ В ОТДЕЛЬНЫХ СТРАНАХ ГЛОБАЛЬНОГО ЮГА 39

§ 1. Понятие и сущность киберпреступлений в отдельных странах Глобального Юга **..... 39**

§ 2. Классификация и типология киберпреступлений в отдельных странах Глобального Юга **..... 53**

§ 3. Особенности криминализации киберпреступлений в отдельных странах Глобального Юга **..... 69**

ГЛАВА II. КРИМИНОЛОГИЧЕСКАЯ ХАРАКТЕРИСТИКА ПРОТИВОДЕЙСТВИЯ КИБЕРПРЕСТУПЛЕНИЯМ В ОТДЕЛЬНЫХ СТРАНАХ ГЛОБАЛЬНОГО ЮГА 96

§ 1. Руководящие документы в сфере противодействия киберпреступлениям в отдельных странах Глобального Юга **..... 96**

§ 2. Институциональные механизмы противодействия киберпреступлениям в отдельных странах Глобального Юга **.....110**

§ 3. Инициативы по противодействию киберпреступлениям в отдельных странах Глобального Юга **..... 126**

ГЛАВА III. УГОЛОВНО-ПРОЦЕССУАЛЬНЫЕ МЕРЫ ПРОТИВОДЕЙСТВИЯ КИБЕРПРЕСТУПЛЕНИЯМ В ОТДЕЛЬНЫХ СТРАНАХ ГЛОБАЛЬНОГО ЮГА 138

§ 1. Особенности расследования киберпреступлений и доказывание в отдельных странах Глобального Юга **..... 138**

§ 2. Наложение ограничительных и иных мер по исполнению антиотмывочного законодательства в отдельных странах Глобального Юга **..... 160**

§ 3. Применение процессуальных мер по исполнению информационного законодательства в отдельных странах Глобального Юга **177**

ГЛАВА IV. МЕЖДУНАРОДНОЕ СОТРУДНИЧЕСТВО В СФЕРЕ ПРОТИВОДЕЙСТВИЯ КИБЕРПРЕСТУПЛЕНИЯМ МЕЖДУ РОССИЙСКОЙ ФЕДЕРАЦИЕЙ И ОТДЕЛЬНЫМИ СТРАНАМИ ГЛОБАЛЬНОГО ЮГА 205

§ 1. Основы международного сотрудничества в сфере противодействия киберпреступлениям между Российской Федерацией и отдельными странами Глобального Юга **205**

§ 2. Проблемы реализации и пути совершенствования регулирования противодействия киберпреступлениям на национальном и региональном уровнях в контексте международного сотрудничества Российской Федерации и отдельных стран Глобального Юга **218**

ЗАКЛЮЧЕНИЕ 232

СПИСОК ИСПОЛЬЗОВАННЫХ СОКРАЩЕНИЙ 239

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ И ЛИТЕРАТУРЫ 244

Приложение № 1. Сравнение аутентичных наименований киберпреступлений с авторским переводом на русский язык **305**

Приложение № 2. Сравнение аутентичных наименований нормативных правовых актов отдельных стран Глобального Юга с официальными переводами на английский язык и авторским переводом на русский язык **307**

Приложение № 3. Сравнение законодательных видов киберпреступлений в отдельных странах Глобального Юга **332**

Приложение № 4. Сравнение положений Будапештской, Арабской и Универсальной конвенций, а также Соглашения ШОС и Конвенции АС **337**

Приложение № 5. Стратегии кибербезопасности на региональном и национальном уровнях **343**

Приложение № 6. Сферы, охватываемые стандартизацией компетентными органами государств-членов ССАГПЗ..... **364**

Приложение № 7. Структура единообразной формы измерения зрелости кибербезопасности (КСА)..... **365**

Приложение № 8. Сравнение аутентичных наименований электронных доказательств с авторским переводом на русский язык..... **367**

ВВЕДЕНИЕ

Актуальность исследования обусловлена, во-первых, постоянно усиливающимся влиянием информационно-коммуникационных технологий на состояние преступности, а во-вторых — абсолютным и относительным ростом числа киберпреступлений, предупреждение, пресечение и расследование которых требует расширения международного сотрудничества. Так, согласно Всемирному индексу киберпреступности 2024 года[1], среди стран пяти континентов корыстная киберпреступность представляет наибольшую угрозу, в первую очередь, для Российской Федерации, что безусловно предполагает необходимость изучения зарубежного опыта и международного сотрудничества в борьбе с ней.

Согласно отчёту Международного союза электросвязи о кибербезопасности 2024 г. к образцовым государствам в сфере обеспечения кибербезопасности, в т.ч. противодействия киберпреступлениям (англ. «*role-modeling*»), относят 47 стран, в частности Королевство Бахрейн (КБ), Арабскую Республику Египет (АРЕ), Республику Индия, Султанат Оман (СО), Государство Катар, Королевство Саудовская Аравия (КСА), Объединённые Арабские Эмираты (ОАЭ), Королевство Марокко (КМ), Иорданское Хашимитское Королевство (ИХК), Республику Индонезия; к продвинутым (англ. «*advancing*») — 29 стран, среди которых Китайская Народная Республика (КНР) и Российская Федерация (РФ); к укрепляющимся (англ. «*establishing*») — 39 стран, среди которых Исламская Республика Иран (ИРИ), Алжирская Народная Демократическая Республика (АНДР), Тунисская Республика (ТР), Федеративная Демократическая Республика Эфиопия (ФДРЭ); к развивающимся (англ. «*evolving*») — 57 стран; к становящимся (англ. «building») — 15 стран[2].

Данное категорирование, безусловно, является динамичным: если арабские страны в 2010-х годах в соответствии с различными индексами кибербезопасности занимали отстающие позиции, с 2020 г. ОАЭ и КСА являются одними из лидеров в

---

[1] Bruce M., Lusthaus J., Kashyap R., Phair N., Varese F. Mapping the global geography of cybercrime with the World Cybercrime Index. PLoS ONE. 2024. №. 19(4). e0297312.

[2] Global Cybersecurity Index. 2024 // ITU. URL: https://www.itu.int/dms_pub/itu-d/opb/hdb/d-hdb-gci.01-2024-pdf-e.pdf (дата обращения: 09.03.2025).

данной области не только среди арабских стран, но и во всём мире. Они занимают соответственно 2-е и 5-е места в рейтинге всемирной кибербезопасности Международного союза электросвязи 2020 г.[3], Саудовская Аравия также занимает 2-е место в мировом индексе кибербезопасности в ежегоднике мировой конкурентоспособности за 2023 г. швейцарского Международного института развития менеджмента[4]. Считается, что арабские монархии, в частности ОАЭ и КСА, имеют потенциал стать «средними цифровыми державами» и одним из их технологических полюсов. Кибербезопасность считается одним из перспективных направлений по сотрудничеству с арабским регионом для Российской Федерации[5].

Большинство из перечисленных ранее стран относится к государствам т.н. Глобального Юга[6], к которым в последнее время теоретики и практики проявляют повышенный интерес. Они входят в различные региональные (не)формальные объединения и международные организации, в частности БРИКС, Шанхайскую организацию сотрудничества (ШОС), Содружество Наций, Лигу арабских государств (ЛАГ), Организацию исламского сотрудничества (ОИС), Совет сотрудничества арабских государств Персидского залива (ССАГПЗ), Африканский союз (АС), Межправительственный орган по развитию (англ. «IGAD»), Ассоциацию государств Юго-Восточной Азии (АСЕАН), тем самым имея уникальное по своей природе нормативное регулирование и институциональные основы противодействия киберпреступлениям и представляя интерес для исследования.

Отсутствие единого подхода к понятию «страны Глобального Юга» к настоящему времени обусловлено многовекторностью международного взаимодействия, которое отражается в данном понятии в измерениях экономики

---

[3] Global Cybersecurity Index 2020 // ITU. URL: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf (дата обращения: 09.03.2025).

[4] Saudi Arabia’s Cybersecurity Recognized as 2nd Best Globally // National Cybersecurity Agency of the Kingdom of Saudi Arabia. 20.06.2023. URL: https://nca.gov.sa/en/news?item=556 (дата обращения: 09.03.2025).

[5] Адрианов А.К. Арабские монархии Персидского залива — новый технологический полюс?: аналитические тезисы № 6 / 2025. М.: Центр Примакова, 2025. С. 4–5.

[6] Яковенко А.В. Картина нарождающегося мира: Глобальный Юг // Проблемы национальной стратегии. 2024. № 1 (82). С. 42–57.

(«догоняющее развитие», «развивающиеся страны», «третий мир» и т.д.), политологии (преодоление колониального наследия и борьба с «лингвистическим империализмом»), юридических документов (где феномен Глобального Юга предполагает точное установление стран, которые могут быть отнесены к данной группе государств по тем или иным — но всегда конкретным — основаниям).

Объединяющий дух «южной солидарности» (англ. «southern solidarity») хорошо проецируется на современные представления о культурном разнообразии, отвечающем концепции многополярного мира. Именно это обеспечивает научную и практическую пользу употребления понятия «страны Глобального Юга» в рамках стратегии развития отношений Российской Федерации с «незападными» странами и партнёрами, представляющими «другой Запад», или Глобальный Север[7].

Поскольку данный феномен прочно вошёл в эвристический багаж науки, но без чётко определённой привязки к конкретным странам (скорее уж регионам), определение рассматриваемых государств остаётся на усмотрение исследователя и опирается в первую очередь на участников БРИКС[8]. Ввиду лидирующих позиций Арабского Востока в обозначенных выше международных индексах кибербезопасности именно он в первую очередь является основой[9], однако для репрезентативности того самого многообразия избраны и те азиатские и африканские страны, с которыми Российская Федерация взаимодействует в рамках обозначенных выше региональных объединений и организаций.

Степень научной разработанности проблемы ныне характеризуется фрагментарностью с упором либо на политическую составляющую (М.А. Сапронова[10]), либо уголовное право и уголовный процесс мусульманских стран в

---

[7] Страны Глобального Юга в среднем насчитывают от 77 до 137 государств в зависимости от научной направленности: политологии, социологии, экономики и эриспруденции. См. подробнее Цыплакова А.Д. Концептуализация понятия «(страны) Глобального Юга»: диффузия повседневной речи, научной терминологии и специализированных дискурсов в призме лингвокультурологии // Концепт: философия, религия, культура. 2025. № 9(2). С. 116-134.

[8] ФДРЭ, ОАЭ, КСА, ИРИ, Республика Индия и КНР.

[9] За основу взяты именно establishing и role-modeling states, согласно отчёту МСЭ 2024 г.

[10] В настоящем исследовании рассматриваются три субрегиона «Арабского Востока»: Африканская (аль-Магрибу (араб. «ٱلْمَغْرِبُ» — запад, закат)), Восточно-средиземноморская (аль-Машрику (араб. «ٱلْمَشْرِقُ» — восток, восход)) и Аравийская (ССАГПЗ) зоны. См. подробнее:

целом (например, Н.А. Аль-Ассуми[11], М. Роэ[12], Джалат Тарват, Сулейман Абдель Аль-Маныйм [13]), либо технические аспекты (e.g., М. Аль-Джассаб [14] , А. Аль-Абдулатиф[15], Ахмад Хамо[16], А. Гешоннек[17]).

Исследованиями отдельных аспектов рассматриваемой проблематики занимаются учёные научной школы МГИМО: в части цифрового права — Э.Л. Сидоренко [18] , В.Ф. Васюков [19] , Э.И.о. Дамирчиев, Е.С. Зиновьева,

---

Сапронова М.А. Арабо-мусульманский мир: история, география, общество: учебное пособие. Казань: Казанский (Приволжский) федеральный университет, 2013. 360 с.

[11] Аль-Ассуми Н.А. Преступление и наказание по уголовному праву Бахрейна и Объединенных Арабских Эмиратов: дис. … канд. юрид. наук: 12.00.08. М., 2000. 161 с.

[12] Роэ М. Исламское право: история и современность / пер. с нем. А. Мухаматчиной; науч. ред. М. Курдатов; под. общ. ред. Д. Мухетдинова. М: Медина, 2019. 576 с.

[13] أصول المحاكمات الجزائية الدعوى الجنائية، سليمان عبد المنعم جلال ثروت. [Джалат Тарват, Сулейман Абдель Аль-Маныйм. Принципы уголовного процесса. Уголовное дело]. Бейрут: Арабский фонд исследований и публикаций, 1996. 641 с.

[14] Alghassab M. Analyzing the Impact of Cybersecurity on Monitoring and Control Systems in the Energy Sector / M. Alghassab // Energies. 2022. № 15 (218). P. 1–21.

[15] Alabdulatif A. Cybercrime and analysis of laws in Kingdome of Saudi Arabia: Science in Information System Security: a thesis for the Master’s Degree / Afnan Alabdulatif; University of Houston. Houston, 2018. 71 p. the Faculty of the Department of Information and Logistics Technology.

[16] Ахмад Хамо, Ала Аваад, Вала Абдулла. Электронные доказательства (юридические и технические аспекты). Палестина: Юридический институт Бирзейтского университета, 2015. 61 с. (на араб. яз.).

[17] Geschonneck A. Computer-Forensik. Computerstraftaten erkennen, ermitteln, aufklären. 5. aktualisierte und erweiterte Auflage. Heidelberg: dpunkt Verlag, 2011.

[18] Сидоренко Э.Л. Право цифровых активов: учебник для бизнеса. М.: Издательский дом «Юрлитинформ», 2025. 312 с.; Международное управление Интернетом / Е. С. Зиновьева, А. А. Игнатов, А. А. Уланов [и др.]. М.: Серпантин Про (ИП Гончаров А.В.), 2025. 186 с.; Цифровой мир: терминологический словарь-справочник в определениях официальных документов / И. Р. Бегишев, И. Р. Альмухамедова, А. К. Арюков [и др.]. Москва: Общество с ограниченной ответственностью «Проспект», 2024. 672 с.; Сидоренко Э. Л. Криптовалюта и будущее цифровых финансов. М.: МГИМО МИД России, 2023. 36 с.; Сидоренко Э. Л. Defi-преступность: состояние, тенденции и криминологические модели // Russian Journal of Economics and Law. 2023. Т. 17, № 2. С. 327-341.

[19] Колычева А.Н., Васюков В.Ф. Расследование преступлений с использованием компьютерной информации из сети Интернет: учебное пособие / под ред. А. Г. Волеводза. Москва: Проспект, 2020. 200 с.; Васюков В.Ф. Противодействие преступлениям в сфере незаконного оборота наркотиков, совершаемым с использованием информационно-телекоммуникационных технологий: учеб. пособие / В.Ф. Васюков, К.К. Клевцов, В.И. Малик; под науч. ред. А.Г. Волеводза. М.: Прометей, 2023. 468 с.; Васюков В.Ф. Преступления в сфере высоких технологий и информационной безопасности: учебное пособие / В.Ф. Васюков, А.Г. Волеводз, М.М. Долгиева, В.Н. Чаплыгина; под науч. ред. А.Г. Волеводза. М.: Прометей, 2023. 1086 с.; Стельмах В.Ю. Производство следственных действий, направленных на получение и использование компьютерной информации: монография / В.Ю. Стельмах, О.М. Ефремова, В.Ф. Васюков / под общ. ред. А. Г. Волеводза. Москва: Проспект, 2021. 480 с.; Васюков В.Ф. Теоретические и правовые аспекты расследования преступлений с использованием абонентской информации:

М.И. Иноземцева, К.К. Таран, Н.Ю. Молчаков[20]; цифровой криминалистики[21] — А.И. Бастрыкин[22]; по вопросам международного сотрудничества в борьбе с преступностью — А.С. Подшибякин[23], А.Г. Волеводз[24], А.В. Гриненко[25],

монография / под ред. докт. юрид. наук А.Г. Волеводза. Орел: Издательство «Картуш», 2020. 339 с.

[20] Цифровое право: учебник / под ред. Э.Л. Сидоренко. М.: Юрлитинформ, 2024. 720 с.

[21] Данной проблематикой также озабочены представители и других школ, в частности МГЮА им. О.Е. Кутафина, Московского университета им. В.Я. Кикотя, Московской академии Следственного комитета им. А.Я. Сухарева, однако комплексные сравнительно-правовые исследования встречаются реже.

[22] Бастрыкин А.И. Выявление и расследование преступлений, совершенных с использованием информационно-коммуникационных технологий // Вестник Российской правовой академии. 2022. № 4. С. 88-94; Бастрыкин А.И. Цифровые технологии современной криминалистики // Вестник Академии Следственного комитета Российской Федерации. 2021. № 2 (28). С. 11-17.

[23] Подшибякин А.С. О технологиях и искусстве в криминалистике // Юридическая техника. 2015. № 9. С. 569-571.

[24] Волеводз А.Г. Противодействие компьютерным преступлениям: правовые основы международного сотрудничества. М.: ООО Издательство «Юрлитинформ», 2002. 496 с.; Волеводз А. Г. Электронные доказательства в уголовном процессе Китайской Народной Республики / А. Г. Волеводз, Ю. Г. Решетников // Вестник экономической безопасности. 2024. № 5. С. 20-27; Волеводз А. Г. Международные правоохранительные организации: Учебное пособие в 5-ти частях / А. Г. Волеводз. М.: ООО «Издательство Прометей», 2023. 224 с. (Библиотека магистратуры «Международное сотрудничество в сфере правоохранительной деятельности и уголовной юстиции»; Часть II; Судебные и юридические сети); Волеводз А. Г. Международные правоохранительные организации. М.: Издательство Проспект, 2011. 344 с.

[25] Уголовный процесс: учебник и практикум. 9-е издание, переработанное и дополненное. М.: Издательство Юрайт, 2024. 361 с.; Криминалистика: учебник / А. В. Гриненко, В. А. Дударев, С. С. Маевский. М.: ООО «Проспект», 2025. 432 с.; Гриненко А. В. Современные проблемы межведомственного взаимодействия следственных органов // Особенности противодействия гибридным угрозам в отношении Российской Федерации: Материалы Луганского международного юридического форума, Луганск, 14 мая 2024 года. Луганск: Луганская академия Следственного комитета Российской Федерации, 2024. С. 51-55; Ivanov D., Grinenko A., Fadeev P., Ermakov S., Antimonova S. Comparative Legal Analysis of the Use of Electronic Format of Criminal Cases and the Procedure under the Code of Criminal Procedure of the Russian Federation // Jurnal Cita Hukum. 2024. Vol. 12, No. 2 P. 309-320.

М.К. Татаринов [26], К.К. Клевцов [27], И.И. Синякин [28], А.Ю. Скуратова [29], И.Н. Кондрат[30]; касательно юридической компаративистики — А.А. Малиновский[31], Е.А. Рыжкова[32], Е.Н. Трикоз[33]; сравнительного правоведения в сфере уголовного права и уголовного процесса — В.В. Дорошков[34], Е.Г. Дубровина, В.В. Дубровин[35]. Несмотря на *prima facie* географическое несоответствие задачам, труды этих учёных стали ценной основой для проводимого исследования.

---

[26] Татаринов М. К. Уголовная юрисдикция в международном уголовном праве. М.: ООО «Издательство Прометей», 2023. 828 с.

[27] Клевцов К. К. Особенности взаимодействия правоохранительных органов с зарубежными поставщиками услуг виртуальных валют (на примере LocalBitcoins) // Вестник Московского университета МВД России. 2023. № 1. С. 139-145; Клевцов К. К. Международное сотрудничество в борьбе с киберпреступностью в контексте противодействия новым вызовам и угрозам // Вестник Санкт-Петербургского университета. Право. 2022. Т. 13. № 3. С. 678-695; Клевцов К.К. Передача уголовного преследования (уголовного судопроизводства) / К.К. Клевцов, А.Г. Волеводз. М.: ООО «Издательство Прометей», 2022. 762 с.

[28] Синякин И.И. Перспективы международно-правового сотрудничества по борьбе с терроризмом // Московский журнал международного права. 2017. № 1(105). С. 78-87.

[29] Международное уголовное право: учебное пособие для специалистов, профессионально занимающихся проблемами борьбы с преступностью / А. Ю. Скуратова, И. И. Синякин. М.: ООО «Проспект», 2025. 560 с.

[30] Иванов И. И. Особенности предупреждения преступлений, совершенных с использованием современных информационно- телекоммуникационных технологий / И. И. Иванов, И. Н. Кондрат // Мировой судья. 2024. № 12. С. 2-9.

[31] Малиновский А.А. История и методология юридической науки. М.: ООО «Издательство Прометей», 2022. 562 с.; Малиновский А.А. Сравнительное уголовное право: учебник. 2-ое издание дополненное и переработанное. М.: Издательство «Юрлитинформ», 2016. 592 с.

[32] Рыжкова Е. А. Становление и развитие права стран Африканского континента: общие вопросы // Право между Востоком и Западом. 2024. № 1. С. 30-38; Рыжкова Е. А. Международное сотрудничество в сфере уголовного судопроизводства: опыт Мальты / Е. А. Рыжкова, С. С. Мельник // Электронное приложение к Российскому юридическому журналу. 2023. № 1. С. 21-26.

[33] Trikoz E. N. Ethical and Legal Landscape of Blockchain in Genetic Research / E. N. Trikoz, N. O. Sidorova, E. E. Gulyaeva // Lex Genetica. 2025. Vol. 4, No. 1. P. 54-66.

[34] Дорошков В. В. К вопросу об уголовном проступке // Мировой судья. 2016. № 12. С. 31-39.

[35] Правовая экспертиза / В. В. Дубровин, А. Г. Волеводз, Е. Г. Дубровина [и др.]. М.: МГИМО, 2024. 364 с.

Отечественные правоведы по исламскому праву в значительной мере сконцентрированы на вопросах финансов, банкинга (например, Р.И. Беккин[36]) или догматики (в частности, Х.В. Идрисов, Л.Р. Сюкияйнен[37]).

Зарубежные учёные зачастую оперируют положениями утративших силу законов или устаревшими их редакциями, поскольку массив работ был написан в 2000–2015 гг. (А. Аль-Кааби, Н. Чантлер, А. МакКуллаг, Г. Мохай, А.А. Кандель[38], Н. Кшетри[39], Ибрагим Халид Мамдух[40], Умар Мухаммад Абу Бакр бин Юнис[41], А.А. Хилали[42], Хишам Мухаммад Харид Растум[43], Харвал Набиль Хиба[44], Р. Нир,

---

[36] Беккин Р.И. Особенности шариатского надзора в исламских финансовых институтах: Современный опыт мусульманских и немусульманских стран // Вестник Санкт-Петербургского университета. Экономика. 2014. № 3. С. 148-164; Беккин Р. И. Исламское или мусульманское право? (К вопросу о правовых аспектах исламских финансов) // Проблемы современной экономики. 2013. № 4(48). С. 429-430.

[37] Сюкияйнен Л. Р. Исламское право и диалог культур в современном мире. 2-ое издание, переработанное. М.: НИУ «Высшая школа экономики», 2025. 680 с.

[38] Alkaabi A., Mohay G., McCullagh A., Chantler N. Dealing with the problem of cybercrime / A. Alkaabi, G. Mohay, A. McCullagh, C. Chantler. // Digital Forensics and Cyber Crime: Second International ICST Conference Revised Selected Papers [Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, 2011, Vol. 53]. Berlin: Springer, 2011. P. 1–18.

[39] Kshetri N. Technological and Global Forces Shaping Cybercrime and Cybersecurity in the Global South / Cybercrime and Cybersecurity in the Global South. London: Palgrave Macmillan, 2013. 250 p.

[40] Ибрагим Халид Мамдух. Искусство уголовного расследования электронных преступлений. 1-ое изд. Александрия: Дом университетской мысли, 2010. 548 с. (на араб. яз.).

[41] Умар Мухаммад Абу Бакр бин Юнис. Преступления, связанные с использованием Интернета.: дисс. … док. юрид. наук. Университет Айн-Шамс. Шарджа, 2004. 885 с. (на араб. яз.).

[42] Хилали А.А. Осмотр компьютерных систем и гарантии киберпреступника: сравнительное исследование. Каир: Дар аль-нахда аль-арабия, 2006. 306 с. (на араб. яз.).

[43] Хишам Мухаммад Харид Растум. Информационные преступления: истоки технического уголовного расследования / Конференция по исследованию права, компьютеров и Интернета в сотрудничестве с Центром стратегических исследований и разработок Эмиратов и Центром информационных технологий при университете: сборник. Аль-Айн: Университет ОАЭ. Колледж шариата и права, 2004. 1145 с. (на араб. яз.).

[44] هروال نبيلة هبة. الجوانب الإجرائية لجرائم الإنترنت في مرحلة جمع الاستدلالات (دراسة مقارنة). ط ١. الإسكندرية: دار الفكر الجامعي، ٢٠٠٧. [Харвал Набиль Хиба. Процессуальные аспекты интернет-преступлений на стадии сбора: сравнительное исследование. 1-ое изд. Александрия: Дом университетской мысли, 2007].

Р. Кларк[45], Аль-Балуши Рашид бин Хамад[46], Аль-Махмуд Али Хамудату[47]). В исследованиях по арабским странам прослеживается порой односторонний подход (например, у З. Ас-Саирафи[48]). Тем не менее есть и ряд более свежих исследований, однако они сосредоточены на конкретной стране (например, Аль-Халиди[49]) или узкоспециализированном регионе (например, Дж. Ширес[50]).

При исследовании избранной темы рассмотрены работы, опубликованные в журналах на иностранных языках, в частности университета короля Сауда (Усамат Ганим Аль-Абэйди[51] и Юнис бин Ахмад Аль-Мушэйкых[52]), Арабского университета наук о безопасности имени принца Наифа (к примеру, К. Мааруф[53]), Исследовательского университета Аль-Истикляль[54] и алжирской базы научных

---

[45] حماية الفضاء الإلكتروني في دول مجلس التعاون لدول الخليج العربية ريتشارد كلارك, روبرت نيك. [Нир Р., Кларк Р. Защита электронного пространства в странах Совета сотрудничества стран Арабского залива]. Emirates Center for Strategic Studies and Research, 2011. 55 с. URL: https://www.ecssr.ae/wp-content/uploads/2019/01/ELS_AR_140.pdf (дата обращения: 01.11.2024).

[46] Аль-Балуши Рашид бин Хамад. Доказательства в информационных преступлениях // Журнал юридического факультета правовых и экономических исследований. 2008. С. 1–58. (на араб. яз.).

[47] Аль-Махмуд Али Хамудату. Доказательства киберпреступлений, умысел и оценка в рамках теории доказательств по уголовным делам [أدلة إثبات الجرائم الإلكترونية ونية وتقديرها في إطار نظرية الاثبات الجنائية] // Журнал безопасности и права. 2003. № 1. С. 9–95.

[48] Al Sairafi Z. Cybersecurity challenges for Human Rights Defenders in Gulf Cooperation Council (GCC) countries: a thesis for a Master's Degree / Zainab Al Sairafi; Central European University. Vienna, 2022.41 p. School of Public Policy.

[49] مبارك بن محمد الخالدي. الإثبات بالدليل الرقمي وتطبيقاته القضائية: دراسة فقهية مقارنة بنظام الإثبات السعودي // مجلة قضاء. ٢٠٢٤. ٣٢٩-٤١٦. [Мубарак бин Мухаммад Аль-Халиди. Доказательство с помощью цифровых доказательств и его судебное применение: юриспруденческое исследование в сравнении с саудовской системой доказательств // Судебный журнал. 2024. С. 329-416 (на араб. яз.).]

[50] Например, Shires J. Ambiguity and appropriation: cybersecurity and cybercrime in Egypt and the Gulf / J. Shires // Governing Cyberspace: Behavior, Power and Diplomacy. Lanham: Rowman & Littlefield, 2020. P. 205–226.

[51] Аль-Абэйди Усамат Ганим. Электронные доказательства в информационных преступлениях // Журнал университета короля Сауда. Право и политология. 2013. № 20 (1). С. 55–82. (на араб. яз.).

[52] يونس بن أحمد المشيقح. مظاهر السلطة التقديرية للنيابة العامة في الدعوى الجزائية وفق الإجراءات الجزائية السعودي [Юнис бин Ахмад Аль-Мушэйкых. Дискреционные полномочия прокуратуры в уголовном деле согласно саудовскому уголовно-процессуальному положению] // Журнал университета короля Сауда. Право и политология. 2020. № 32 (2). С. 245–262.

[53] Maarouf K. Procedural Problems Facing a Criminal Investigator in Cybercrimes // Arab Journal of Forensic Sciences and Forensic Medicine. 2022. № 4 (2). P. 158–166 (in Arabic).

[54] عدنان إبراهيم الحجار، فايز خضر بشير. الأدلة الرقمية وإثبات الجرائم السيبرانية ما بين التأصيل والتأويل [Аднан Ибрагим Аль-Хаджар, Файез Хедр Башир. Цифровые улики и доказательства киберпреступлений: между укоренением и интерпретацией] // Журнал Исследовательского университета Аль-Истикляль. 2021. № 6 (1). С. 129–152.

журналов на арабском языке, «Сравнительное уголовное правоведение» [55], «Судебный журнал» на персидском языке, которые тем не менее носят фрагментарный характер.

За последние 20 лет были защищены смежные с темой исследования диссертации на соискание ученой степени кандидата юридических наук по отдельным направлениям уголовно-правовых наук (12.00.08, 12.00.09, 12.00.12) и с опорой преимущественно на отечественную практику и опыт либо ограничением одной–двумя странами: К.В. Костомаровым[56], Р.С. Атамановым[57], А.Н. Ягудиным[58], В.В. Челноковым[59], В.О. Давыдовым[60], И.Г. Чекуновым [61], А.И. Кананович [62],

---

[55] هادی تبار, اسماعیل, یعقوبی گلوردی, محمد کاظم. ادله اثبات الکترونیکی در دادرسی‌های کیفری در نظام حقوقی ایران // فقه جزای تطبیقی. ۲۰۲۳. ۳ (۱). ۱۲۳-۱۱۳. [Хади Табар, Исмаил, Якуби Глорди, Мохаммад Казем. Доказательства электронных доказательств в уголовном процессе в правовой системе Ирана // Сравнительное уголовное правоведение. 2023. № 3 (1). С. 113-12].

خسروی زاد, افشار, سپهری, روح الله, بابایی, حمیده. مشروعیت تحصیل دلیل در جرایم فضای مجازی در حقوق جزایی ایران // فقه جزای تطبیقی. ۲۰۲۲. ۲ (۳). ۷۵-۸۵ [Хосравизад, Афшар, Сепери, Рухолла, Бабаи, Хамида. Легитимность изучения доказательств преступлений в киберпространстве в уголовном праве Ирана // Сравнительное уголовное правоведение. 2022. № 2 (3). С. 75-85],

احسان پور, سید رضا, امی, احمد. جرایم «فناوری جعل عمیق» از منظر فقه و حقوق کیفری // فقه جزای تطبیقی. ۲۰۲۲. ۲ (۴). ۱-۹ [Эхсанпур, Сейед Реза, Эми, Ахмед. Преступления «технологии дипфэйка» с позиций юриспруденции и уголовного права // Сравнительное уголовное правоведение. 2022. № 2 (4). С. 1-9].

[56] Костомаров К.М. Первоначальный этап расследования преступлений, связанных с незаконным доступом к компьютерной информации банков: дис. ... канд. юрид. наук: 12.00.09.- Екатеринбург, 2012. 212 с.

[57] Атаманов Р.С. Основы методики расследования мошенничества в сети Интернет: дис. ... канд. юрид. наук: 12.00.09. М., 2012. 182 с.

[58] Ягудин А.Н. Уголовная ответственность за нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей: дис. ... канд. юрид. наук: 12.00.08. М., 2013. 201 с.

[59] Челноков В.В. Компьютерная информация как предмет преступления в отечественном уголовном праве: дис. ... канд. юрид. наук: 12.00.08. Екатеринбург, 2013. 226 с.

[60] Давыдов В.О. Информационное обеспечение раскрытия и расследования преступлений экстремистской направленности, совершенных с использованием компьютерных сетей: дис. ... канд. юрид. наук: 12.00.12. Тула, 2013. 264 с.

[61] Чекунов И.Г. Криминологическое и уголовно-правовое обеспечение предупреждения киберпреступности: дис. ... канд. юрид. наук: 12.00.08. Москва, 2013.223 с.

[62] Кананович А.И. Уголовно-правовая защита авторских прав в глобальной сети Интернет (на примере законодательств России и Франции): дис. ... канд. юрид. наук: 12.00.08. Москва, 2013. 229 с.

О.М. Сафоновым[63], А.С. Вражновым[64], Е.С. Шевченко[65], М.А. Простосердовым[66], В.Г. Степановым-Егиянцом [67], В.В. Коломиновым [68], А.С. Щуровой [69], И.Е. Мазуровым[70], Р.Р. Гайфутдиновыи [71], Н.В. Летёлкиным[72], А.Н. Колычеваой[73], М.Д. Фроловым[74], А.А. Дрога[75], О.А. Решняк[76], В.А. Жаворонковым[77], А.С. Камко[78],

---

[63] Сафонов О.М. Уголовно-правовая оценка использования компьютерных технологий при совершении преступлений: состояние законодательства и правоприменительной практики, перспективы совершенствования: дис. ... канд. юрид. наук: 12.00.08. Москва, 2015. 222 с.

[64] Вражнов А.С. Криминалистический риск при расследовании неправомерного доступа к компьютерной информации: дис. ... канд. юрид. наук: 12.00.12. Москва, 2015. 218 с.

[65] Шевченко Е.С. Тактика производства следственных действий при расследовании киберпреступлений: дис. ... канд. юрид. наук: 12.00.12. Москва, 2016. 249 с.

[66] Простосердов М.А. Экономические преступления, совершаемые в киберпространстве, и меры противодействия им: дис. ... канд. юрид. наук: 12.00.08. Москва, 2016. 232 с.

[67] Степанов-Егиянц В.Г. Методологическое и законодательное обеспечение безопасности компьютерной информации в Российской Федерации (уголовно-правовой аспект): дис. ... док. юрид. наук: 12.00.08. Москва, 2016. 389 с.

[68] Коломинов В.В. Расследование мошенничества в сфере компьютерной информации: научно-теоретическая основа и прикладные аспекты первоначального этапа: дис. ... канд. юрид. наук: 12.00.12. Краснодар, 2017. 211 с.

[69] Щурова А.С. Незаконный оборот наркотических средств и их аналогов с использованием компьютерных технологий (сети Интернет): уголовно-правовое и криминологическое исследование: дис. ... кандидата юридических наук: 12.00.08. Санкт-Петербург, 2017. 256 с.

[70] Мазуров И.Е. Методика расследования хищений, совершенных с использованием Интернет-технологий: дис. ... канд. юрид. наук: 12.00.12. Ростов: 2017. 188 с.

[71] Гайфутдинов Р.Р. Понятие и квалификация преступлений против безопасности компьютерной информации: дис. ... канд. юрид. наук: 12.00.08. Казань, 2017. 243 с.

[72] Летёлкин Н.В. Уголовно-правовое противодействие преступлениям, совершаемым с использованием информационно-телекоммуникационных сетей (включая сеть «Интернет»): дис. ... канд. юрид. наук: 12.00.08. Нижний Новгород, 2018. 218 с.

[73] Колычева А.Н. Фиксация доказательственной информации, хранящейся на ресурсах сети Интернет: дис. ... канд. юрид. наук: 12.00.12. Москва, 2019. 199 с.

[74] Фролов М.Д. Уголовно-правовое и криминологическое противодействие мошенничеству в сфере компьютерной информации: дис. ... канд. юрид. наук: 12.00.08. Москва, 2019. 211 с.

[75] Дрога А.А. Развитие методики судебно-бухгалтерских экспертиз на основе данных, сопряженных с использованием компьютерных средств: дис. ... канд. юрид. наук: 12.00.12. Москва, 2019. 253 с.

[76] Решняк О.А. Использование компьютерных технологий при расследовании преступлений в сфере незаконного оборота опасных психоактивных веществ: дис. ... канд. юрид. наук: 12.00.12. Волгоград, 2020. 220 с.

[77] Жаворонков В.А. Информационно-компьютерное обеспечение судебной экспертизы маркировочных обозначений транспортных средств: дис. ... канд. юрид. наук. Москва, 2020. 268 с.

[78] Камко А.С. Предупреждение мошенничества с использованием телекоммуникационных и компьютерных сетей: дис. ... канд. юрид. наук: 12.00.08. Владивосток, 2020. 228 с.

Н.С. Зиновьевой[79], Г.Р. Григоряном[80], О.М. Ефремовой[81], А.Г. Себякиным[82], Е.А. Кот[83], Д.В. Завьяловой[84], К.Н. Евдокимовым[85], А.В. Кутузовым[86].

После укрупнения специальности (5.1.4) ситуация осталась практически неизменной: И.С. Мочалкина[87], А.С. Ильницкий[88], Е.А. Родин[89], М.Н. Турунова[90],

[79] Зиновьева Н.С. Компьютерная информация, преобразованная методами криптографии, в раскрытии и расследовании преступлений: дис. ... канд. юрид. наук: 12.00.12. Краснодар, 2021. 207 с.

[80] Григорян Г.Р. Мошенничество в сфере компьютерной информации: проблемы криминализации, законодательной регламентации и квалификации: дис. ... канд. юрид. наук: 12.00.08. Самара, 2021. 243 с.

[81] Ефремова О.М. Реализация полномочий следователя, направленных на получение и использование компьютерной информации при производстве следственных действий: дис. ... канд. юрид. наук: 12.00.09. Орел, 2021. 225 с.

[82] Себякин А.Г. Тактика использования знаний в области компьютерной техники в целях получения криминалистически значимой информации: дис. ... канд. юрид. наук: 12.00.12. Москва, 2021. 271 с.

[83] Кот Е.А. Расследование преступлений, совершенных в сети Интернет, связанных с побуждением несовершеннолетних к суициду: дис. ... канд. юрид. наук: 12.00.12. Калининград, 2022. 326 с.

[84] Завьялова Д.В. Расследование преступлений в сфере компьютерной информации: отечественный и зарубежный опыт: дис. ... канд. юрид. наук: 12.00.12. Москва, 2022. 242 с.

[85] Евдокимов К.Н. Противодействие компьютерной преступности: теория, законодательство, практика: дис. ... док. юрид. наук: 12.00.08. Москва, 2022. 557 с.

[86] Кутузов А.В. Методологические основы раскрытия и расследования преступлений экстремистской направленности с использованием информационно-телекоммуникационной сети Интернет: дис. ... канд. юрид. наук: 12.00.12. Ростов-на-Дону, 2022. 237 с.

[87] Мочалкина И.С. Цифровые права и цифровая валюта как предмет преступлений в сфере экономики : дис. ... канд. юрид. наук: 5.1.4. Москва, 2022. 240 с.

[88] Ильницкий А.С. Противодействие криминальной идеологии в сети Интернет: дис. ... канд. юрид. наук: 5.1.4. Краснодар, 2022. 213 с.

[89] Родина Е.А. Противодействие криминальной виктимизации пользователей сети «Интернет» в киберпространстве: дис. ... канд. юрид. наук: 5.1.4. Саратов, 2022. 217 с.

[90] Турунова М.Н. Противодействие влиянию сети «Интернет» на преступное поведение несовершеннолетних: дис. ... канд. юрид. наук: 5.1.4. Санкт-Петербург, 2023. 242 с.

В.А. Туркулец [91], Г.Ф. Шипулин[92], Е.А. Харина[93], Н.А. Столбова [94], В.С. Асламова [95], М.М. Льянов[96], Л.Л. Бошаева[97].

Указанные научные труды послужили основой настоящего диссертационного исследования. Признавая их теоретическую значимость в контексте исследования проблематики противодействия киберпреступлениям, в свете отсутствия единого целостного подхода и существования ряда неразрешенных вопросов, существует необходимость продолжения уголовно-правовых исследований в этой сфере.

Целью диссертационного исследования является формирование комплексного представления о правовых проблемах, возникающих при противодействии киберпреступлениям в отдельных странах Глобального Юга, а также о путях их решения в контексте сотрудничества с ними Российской Федерации для сближения правовых систем (правовой конвергенции).

Для достижения заявленной цели определены ***следующие задачи исследования***:

1) сконструировать теоретическую модель киберпреступлений, предусмотренных регулированием отдельных стран Глобального Юга;

---

[91] Туркулец В.А. Защита несовершеннолетних от преступных посягательств, совершаемых с использованием сети Интернет: дис. ... канд. юрид. наук: 5.1.4. Москва, 2024. 249 с.

[92] Шипулин Г.Ф. Предупреждение преступлений, совершаемых с использованием компьютерных сетей: дис. ... канд. юрид. наук: 5.1.4. Москва, 2024. 201 с.

[93] Харина Е.А. Особенности методики расследования мошенничества в сфере компьютерной информации: дис. ... канд. юрид. наук: 5.1.4. Краснодар, 2024. 248 с.

[94] Столбова Н.А. Методика расследования незаконного оборота огнестрельного оружия с использованием информационно-телекоммуникационных сетей, в том числе сети «Интернет»: дис. ... канд. юрид. наук: 5.1.4. Иркутск, 2024. 243 с.

[95] Асламова В.С. Оперативно-розыскное противодействие преступлениям, совершаемым в сфере незаконного оборота наркотиков с использованием сети «Интернет» на территории Российской Федерации и Республики Казахстан (сравнительно-правовое исследование): дис. ... канд. юрид. наук: 5.1.4. Санкт-Петербург, 2024. 168 с.

[96] Льянов М.М. Криминалистическое значение электронно-цифровых следов преступлений экстремистской и террористической направленности в сети "Интернет": дис. ... канд. юрид. наук: 5.1.4. Екатеринбург, 2025. 248 с.

[97] Бошаева Л.Л. Предупреждение киберпреступности в отношении несовершеннолетних": дис. ... канд. юрид. наук: 5.1.4. Москва, 2025. 259 с.

2) проанализировать существующие классификации и типологии кибердеяний в изучаемых государствах в преломлении преступности, наказуемости и мер противодействия;

3) выявить особенности криминализации и пенализации киберпреступлений в государствах Глобального Юга для осуществления эффективного международного сотрудничества;

4) раскрыть положения руководящих документов в сфере кибербезопасности обозначенных стран для оценки сложившихся тенденций;

5) систематизировать разработанные институциональные механизмы по противодействию киберпреступлений в вышеупомянутых государствах для возможного имплементирования в России;

6) выделить наиболее эффективные инициативы по противодействию киберпосягательствам и предложить их для внедрения в отечественное регулирование;

7) установить трудности при определении правового статуса цифровых (электронных) [98] доказательств и процессуального порядка их закрепления в рассматриваемых государствах;

8) изучить и оценить действующие ограничительные меры по исполнению антиотмывочного законодательства в отдельных странах и порядок их наложения в приложении к виртуальному пространству;

9) обозначить и сопоставить процессуальные меры по исполнению информационного законодательства в исследуемых государствах и порядок их применения;

10) определить основы международного сотрудничества в сфере противодействия киберпреступлениям между Россией и странами Глобального Юга и правовые проблемы при его осуществлении;

11) выработать рекомендации по совершенствованию существующего регулирования противодействия киберпреступлениям на национальном и

[98] В аутентичных текстах и на практике данные понятия являются взаимозаменяемыми, хотя и имеют разные оттенки.

региональном уровнях в контексте сотрудничества Российской Федерации с государствами Глобального Юга.

Объектом исследования являются общественные отношения, складывающиеся в сфере противодействия киберпреступлениям[99] в отдельных странах Глобального Юга.

Предмет настоящего исследования составляют действующие правовые нормы отдельных отраслей права, которые регулируют отношения в сфере противодействия киберпреступлениям в некоторых государствах Глобального Юга: в Объединённых Арабских Эмиратах, Королевстве Саудовская Аравия, Королевстве Бахрейн, Государстве Кувейт, Государстве Катар, Арабской Республике Египет, Алжирской Народной Демократической Республике, Тунисской Республике, Королевстве Марокко, Иорданском Хашимитском Королевстве, Исламской Республике Иран, Федеративной Демократической Республике Эфиопия, Республике Индия, Республике Индонезия, Китайской Народной Республике[100], универсальное и региональное регулирование на уровне ЛАГ, ССАГПЗ, Содружества Наций[101], Совета Европы[102], ШОС, БРИКС, ОИС, АС, АСЕАН, IGAD, ООН, практика их правоприменения, научные теории, имеющие отношение к рассматриваемой проблематике, доктринальные исследования российских и иностранных учёных, а также экспертные оценки в исследуемой сфере.

Хронологические рамки исследования охватывают период с 2000-х годов, когда принимались первые нормативные правовые акты в сфере противодействия

---

[99] Поскольку в аутентичных текстах законодательств и в доктрине нет единообразного подхода к терминологии, а в официальных переводах на английский язык исключительным образом используется термин «киберпреступления» (анг. «cybercrimes») и международный договор ООН принят в редакции «Конвенция против киберпреступности …», именно данное понятие взято за основу за исключением тех случаев, когда используются термины, специфичные для конкретной правовой системы.

[100] С учётом широты понятия стран Глобального Юга перечисленные государства отражают основные тенденции и стандарты, применимые в том числе и к странам, которые не охвачены исследованием.

[101] Релевантно в контексте Республики Индия.

[102] Несмотря на то, что Россия более не является членом СЕ, а рассматриваемые страны и не являлись таковыми, некоторые из них являются подписантами международных договоров данной организации и участниками её программ.

киберпреступлениям в обозначенных государствах Глобального Юга, по настоящее время.

Методология и методы исследования. Методологическую основу исследования составляют общенаучные и частные методы познания, в том числе социальные и специально-юридические. Проведённое исследование, во-первых, основано на таких общенаучных методах познания, как диалектический метод (при определении общего направления исследования), методы формальной логики (анализ, синтез, индукция, дедукция, аналогия), системный метод (при сопоставлении и обобщении результатов исследования), а также классификации и описание, исторический и прогностический методы при ретроспективной и перспективной оценках состояния кибербезопасности и регулирования рассматриваемых стран и сотрудничества с Российской Федерацией.

Во-вторых, в ходе написания работы применены контент-анализ документов эмпирической базы, уголовно-статическое изучение (в отношении совершенных киберпреступлений), изучение экспертных оценок преступности (позиций теоретиков и практиков), моделирование.

В-третьих, при изучении нормативных правовых актов, стандартов и руководств органов государственной власти отдельных государств[103] использованы специально-юридические методы: толкование, формально-юридический, историко-правовой методы, а также методы юрислингвистики и лингвоюристики в части языковых особенностей использования терминов правоприменителями, законодателями и исследователями на иностранных языках (английском, французском, китайском, арабском, персидском, амхарском, индонезийском, португальском). Исследование носит сравнительный характер и построено на микро- и макросравнении, синхронном и диахронном, внешнем и внутреннем, доктринальном, нормативном и проблемном сравнениях. При выявлении

[103] Даты документов в арабских странах зачастую указаны в оригинале по исламскому календарю (лунная хиджра); в ИРИ — солнечная хиджра, основывающаяся на тропическом годе. Ведётся счёт от 16.07.622 н.э. — переселения пророка Мухаммада из Мекки в Медину (араб. «هجرة»). Для единообразия все даты переведены в григорианский календарь.

противоречий, недостатков и пробелов в законодательстве и иных источниках права использован критико-правовой метод.

Выборка стран основывается на стратегическом отборе случаев через типичные, разнообразные, экстремальные, девиантные, влиятельные, наиболее похожие и самые разные случаи[104]. Так называемый дизайн наиболее различных систем, основанный на методе исследования причинных связей (Ф. Бэкона и Дж. Милля), показывает, что максимально различные контексты, давая схожие результаты, свидетельствуют о наличии устойчивых закономерностей [105] . Избранные страны отличаются по ключевым показателям: политический режим, уровень экономического и технологического развития, цифровизации и кибербезопасности, правовая система (принадлежность к правовой семьи), участие в международных договорах, государственный контроль и нормативно-правовая база[106] — для внутрирегионального анализа и глобальной сопоставимости через конфигурационный подход[107] и анализ отклоняющихся случаев[108].

Теоретическую базу настоящей диссертации составили работы отечественных и зарубежных юристов-учёных из различных отраслей уголовно-правовых наук, в частности уголовного материального права, уголовного процесса, криминалистики, криминологии, международного уголовного права. При изучении юрислингвистических особенностей терминологии использованы труды

---

[104] См. подробнее о методе Seawright J., Gerring J. Case Selection Techniques in Case Study Research // Political Research Quarterly. 2008. № 61. P. 294-308.

[105] См. подробнее о методе Przeworski A., Teune H. The Logic of Comparative Social Inquiry. Wiley-Interscience, 1970. 153 p.

[106] В основном взяты за основу показатели отчёта Международного союза электросвязи о кибербезопасности 2024 г.

[107] См. подробнее о методе Ragin C.C. The Comparative Method: Moving Beyond Qualitative and Quantitative Strategies. Berkeley: University of California Press, 1989. 218 p.

[108] См. подробнее о методе Seawright J., Gerring J. Указ. Соч.

филологов и лингвистов, в особенности по арабскому [109], персидскому [110], амхарскому[111], индонезийскому[112] языкам (школы МГИМО МИД России и РАН).

Нормативно-правовую базу диссертационного исследования составили национальные законы на уровне федерации, субъектов, специальных административных районов, особых экономических (свободных финансовых) зон, специальных экономических городов и зон, промышленных городов и технологических зон, подзаконные акты, принятые на уровне высших должностных лиц, государственных органов и их структурных подразделений зарубежных стран (ОАЭ, КСА, КБ, СО, Государства Кувейт, Государства Катар, АРЕ, АНДР, ИХК, ТР, КМ, КНР, Республик Индия, Индонезия, ИРИ, ФДРЭ) и прямо или косвенно касающихся вопросов кибербезопасности, а также двусторонние и многосторонние международные договоры в сфере борьбы с преступностью.

Эмпирическая и информационная база исследования включает судебную практику судов арабских стран, Ирана, КНР, Республик Индия и Индонезия апелляционной и кассационной инстанций, официальные данные, руководящие и рекомендательные документы органов государственной власти рассматриваемых государств, отчёты и заметки юридических, технических и правозащитных организаций, новостные сводки и интервью представителей государственной власти из изданий, широко тиражируемых в рассматриваемых странах Глобального Юга, а также декларации, дорожные карты, стратегии регионального уровня.

---

[109] Например, Баранов Х.К. Большой арабско-русский словарь в 2-х томах. М.: Русский язык, 2006. 1450 с.; Яковенко Э.В. Арабский язык. Практический курс перевода: учебное пособие / Э.В. Яковенко. М.: Издательство восточной литературы, 2019. 464 с.; Яковенко Э.В. Арабский язык для юристов-международников. Часть 1: Учебник / под ред. А.А. Малиновского, Н.М. Шуйской. М.; Прометей, 2025. 392 с.

[110] В частности, Иванов В.Б. Большой персидско-русский словарь: около 76000 слов, 61000 фразеологизмов и примеров: в трех томах. М.: Фонд Ибн Сины, 2023. 1903 с.; Рубинчик Ю.А. Грамматика современного персидского литературного языка / под ред. М.И. Карповой. М.: Восточная литература РАН, 2001. 600 с.; Островенко Е.Д. Русско-персидский словарь дипломатической лексики: более 10 тысяч слов и словосочетаний на русском, персидском и дари языках. 2-е издание, переработанное и дополненное. М.: МГИМО-Университет, 2020. 698 с.

[111] Завадская Е.П. Учебный словарь новой лексики амхарского языка / Е.П. Завадская М.: МГИМО-Университет, 2012. 300 с.; Завадская Е.П. Амхарский язык. Общественно-политический перевод / Е.П. Завадская М.: МГИМО-Университет, 2011. 345 с.

[112] Индонезийский язык для международников = Bahasa Indonesia untuk hubungan internasional. Учебник / под ред. Н.А.Толмачёв. М.: МГИМО-Университет, 2014. 291 с.

Научная новизна диссертации заключается в первом комплексном исследовании правовых проблем противодействия киберпреступлениям в обозначенных странах Глобального Юга как стратегических партнёров Российской Федерации и международного сотрудничества с ними в этой сфере в сравнительном ключе. Оно в свою очередь объединяет основные направления уголовно-правовых наук (уголовное право, уголовный процесс, криминология, криминалистика, международное сотрудничество в сфере борьбы с преступностью), что в полной мере корреспондирует укрупнению научных специальностей Высшей аттестационной комиссии под шифром «5.1.4. Уголовно-правовые науки» и делает его уникальным. Избранный сравнительный подход, предмет и методология позволили следующее:

- установить уголовно-правовое содержание киберпреступлений;

- определить направления стратегических документов и эффективные организационные и технические меры предупреждения кибердеяний;

- охарактеризовать надлежащее обеспечение расследования и доказывания киберпосягательств, наложения процессуальных мер по исполнению информационного и антиотмывочного законодательства;

- сформулировать предложения по совершенствованию внутригосударственного регулирования и межгосударственного взаимодействия.

По результатам проведенного исследования выносятся следующие ***положения на защиту*** диссертации на соискание учёной степени кандидата юридических наук.

1. Ввиду цифрового разрыва, неравномерного развития технологий и, как следствие, различного нормативного регулирования отдельных стран Глобального Юга, не определены единообразные подходы к противодействию киберпреступлениям. Несмотря на многообразие понятийного аппарата на иностранных языках, в качестве понятия общего рода выступают именно киберпреступления. С учётом генезиса норм, криминализующих и пенализующих указанные деяния в странах Глобального Юга, и юрислингвистических особенностей понимание рассматриваемого вида прошло путь от экономических

компьютерных преступлений (узкий подход в 2000-х и первой половине 2010-х гг.) до использования информационных технологий в преступных целях (широкий подход во второй половине 2010-х и 2020-х годах).

Даже в рамках одного региона (будь то арабского, азиатского или африканского) нет единой позиции ни при определении, ни при наполнении содержания рассматриваемых посягательств. Под киберпреступлениями в странах Глобального Юга предлагается понимать запрещённые законом деяния, совершаемые в отношении или с использованием данных, информационных (компьютерных) сетей и систем, личность (честь и её достоинство), цифровых объектов (документов идентификации, в том числе подписей, печатей и сертификатов, электронных средств платежа и виртуальных активов, электронных документов), прав интеллектуальной собственности, охраняемых законом тайн, а также правонарушения регулирования телекоммуникационного сектора, лицензируемых видов деятельности, оказания сертифицированных услуг, правил пользования социальными сетями, мессенджерами, средствами связи и публикаций, в том числе электронной рекламы и контента, электронного документооборота в государственном и частном секторах, обеспечения безопасности объектов критической (информационной) инфраструктуры, удалённой работы, оказания государственных услуг, электронного голосования, электронной торговли, юридической деятельности и интересов потребителей — корреспондируя делению на посягательства с кибервозможностями и киберзависимые преступления.

Тем не менее существующим киберрегулированием стран Глобального Юга не запрещены отдельные вызовы и угрозы, такие как мета-преступления, цифровые наркотики, электронные мухи, посягательства на внутриигровые активы, использование искусственного интеллекта в преступных целях, кибертерроризм, что может быть предметом отдельных законопроектов, дополнительных протоколов или международных договоров в дальнейшем. С опорой на сложившуюся типологию киберпреступлений и универсальные формулировки необходимо адаптировать уголовный, уголовно-процессуальный и смежные акты

таким образом, чтобы закон стал инструментом, не догоняющим преступность, а опережающим её.

Автором предлагается универсальное определение киберпреступлений — использование высоких технологий в преступных целях.

2. Ввиду трансграничного характера и технических особенностей киберпреступлений особое значение приобретают соблюдение принципа двойной криминальности и установление уголовной юрисдикции государства в виртуальном пространстве. С учётом «цифровизации» понятия места совершения преступления возникают предпосылки для конфликта юрисдикций (на межгосударственном уровне), подсудности и подследственности (на внутригосударственном уровне) и, как следствие, развития новых юрисдикционных привязок. Примерами таковых служат ИРИ, КНР (относительно новаторские), Республика Индия, АНДР и Тунис (развитие традиционных).

В качестве новых юрисдикционных привязок предлагается использовать принадлежность домена верхнего уровня веб-сайта с кодом конкретной страны, места расположения серверов Интернет-ресурсов, используемых для осуществления преступной деятельности, местоположение поставщиков сетевых услуг, местонахождение нарушенных информационных сетевых систем и их менеджеров, а равно информационных сетевых систем, которые использовались подозреваемыми, обвиняемыми или потерпевшими, места, где потерпевшим нанесен вред или где имели место потери имущества, гражданство лица, которому принадлежат данные, а также территории хранения, обработки, скрининга или федерализации данных и территориальное расположение использованных при совершении преступления компьютерных ресурсов.

3. Наряду с законодательным, выделяются доктринальный и правоприменительный подходы к классификации киберпреступлений. При этом национальное регулирование и международно-правовые документы оказали друг на друга взаимопроникающее влияние, хотя и в ограниченном виде с учётом стремления стран Глобального Юга сохранять свою идентичность. Позиции государств именно Глобального Юга, высказанные при разработке Универсальной

конвенции, и национальное киберрегулирование стоит положить в основу дополнительных протоколов и новых международных договоров.

4. Противодействие киберпреступлениям — это комплексная деятельность правоохранительных и специализированных государственных органов, органов законодательной и судебной властей, должностных лиц, физических и юридических лиц (и подобных им корпоративных образований) на горизонтальном и вертикальном, внутри- и межгосударственном уровнях, включающая разработку нормативных правовых актов, стандартов, руководств и стратегий, профилактические (просветительские), экономико-технические и пресекательные инициативы, борьбу с киберпосягательствами (выявление, раскрытие, расследование кибердеяний, уголовное преследование за них, в том числе наложение ограничительных, обеспечительных и иных процессуальных мер) и осуществление в связи с этим международного сотрудничества в двустороннем и многостороннем форматах.

5. С учётом данного определения развитие противодействия киберпреступлениям на внутригосударственном и межгосударственном уровнях разнятся. На региональном уровне в первую очередь утверждаются стратегические документы, призванные объединить усилия не только (и не сколько) в борьбе с киберпреступностью, но и сокращении т.н. цифрового разрыва, порой по времени опережая (азиатский регион) или отставая от национального уровня (арабский и африканский регионы), а также создаются институциональные механизмы (министерские встречи, рабочие группы, исполнительные комитеты и CERT) по кибертематике (цифровой трансформации, электронным торговле и правительстве), противодействию преступности в целом (полицейские службы и конференции по исполнению конвенций).

На национальном же уровне руководящие документы носят скорее секторальный характер, отражая основные тенденции, и принимаются органами, которые преобразованы из структурных подразделений в самостоятельные единицы с расширенной компетенцией, в том числе по координации деятельности, разработке нормативного и технического регулирования, научно-

исследовательских и просветительских проектов, а также вспомогательными функциями при расследовании инцидентов и преступлений. Сферой деятельности являются развитие человеческих ресурсов и технической оснащённости, выявление талантов, укрепление этического использования ИТ, повышения киберосознанности и кибергигиены населения, а также международное сотрудничество и государственно-частное партнёрство. Среди специализированных органов (в широком смысле) выделяются как непосредственно, так и опосредованно участвующие в уголовном судопроизводстве.

6. Государственное устройство отдельных стран Глобального Юга и их экономические потребности способствуют развитию гибкой нормативно-правовой базы и бюрократического аппарата с особыми полномочиями в рамках субъектов и территорий со специальными режимами, то есть специальных зон (особые экономические или свободные финансовые зоны, промышленные города, технические зоны, специальные экономические города и зоны) и районов (специальные административные районы КНР). Первоначально не обладающие функциями по уголовному преследованию компетентные комиссии, комитеты и инспекторы (должностные лица исполнительной власти) могут фиксировать правонарушения, в том числе уголовно наказуемые, формировать отчёты, собирать криминалистически значимую информацию (в отдельных случаях — доказательства) и проводить неотложные следственные и иные процессуальные действия (обыски, выемки, аресты, участвовать в наложении обеспечительных мер). В отдельных странах Глобального Юга существует тенденция привлечения обладающих специальными познаниями должностных лиц из конкретных министерств и ведомств, что целесообразно предусмотреть в отечественном регулировании и использовать на практике.

7. Киберпространство способствует размытию привычных границ в праве: единство субъекта и объекта правоотношений, сочетание начал уголовной и административной ответственности и, как следствие, множественность компетентных органов, налагающих наказание, применимость гражданского и

гражданского процессуального права в качестве *lex specialis*. Однако это не предопределяет полисемантичность (полисемию) используемых терминов с добавлением киберсоставляющей, а требует сбалансированного и обоснованного подхода при их «цифровизации», в том числе имущества, отдельных объектов оборота, места совершения преступления (происшествия), ущерба, наказаний и иных.

8. Понятийный аппарат в части доказательств характеризуется устойчивостью, хотя даже в одном государстве может быть непоследовательным. Условно термины «электронный», «цифровой» и «компьютерный» соотносятся как общее и частное, однако предполагается их использование в качестве синонимов. Несмотря на всю дискуссионность цифровых доказательств как таковых, *de facto* доказательства в электронном виде давно признаны в рамках уголовного судопроизводства (исходя из принятых принципов и выработанной судебной практики), *de jure* — зависит от облекаемой формы и регламентации правового статуса: самостоятельный вид, приравнивание носителя информации к письменным документам, вещественные доказательства, полученные в ходе судебной экспертизы. Сходным образом произошло и с использованием иных технологических достижений, например видеоконференцсвязи. Вдобавок, не только активно обсуждаются, но уже и применяются специализированные информационные системы для уведомлений и получения судебных решений, электронного документооборота, Блокчейн для обеспечения целостности доказательств и отслеживания цепочки хранения, искусственного интеллекта при обработке большого массива данных. Всё это должно учитываться при организации международного сотрудничества в сфере уголовного судопроизводства и возможной имплементации в отечественный уголовный процесс.

9. Трудности в получении электронных доказательств кроются не столько в техническом компоненте (который, несомненно, также играет важную роль), сколько в контрасте процедур даже в рамках одного региона: обыск, выемка, изъятие, перехват контента, прослушивание, контроль сообщений, наблюдение, дистанционные и физические «цифровые расследования», электронный

мониторинг, извлечение и копирование данных производятся как с судебным решением, так и без него. При этом отсутствие деления на оперативно-розыскные мероприятия и следственные действия и открытый перечень последних (например, в арабских странах) способствует гибкости процесса получения и фиксации доказательственной информации и дополняется расширенным перечнем лиц, привлекаемых для производства процессуальных действий. Нарушение обязанности сотрудничать может влечь наложение юридической ответственности, вплоть до уголовной. Относительно высокая степень регламентации оформления документов и изъятых предметов с фото- и видеофиксацией объясняется развитой системой как подзаконных актов, так и руководств (белых книг), составленных теоретиками и практиками.

10. Действующим зарубежным законодательством охватываются данные о содержании (контенте), трафике, учете преобразования частных сетевых адресов в публичные сети, конечном оборудовании, технических характеристиках, дате, времени и продолжительности соединения, дополнительных услугах, посещённых Интернет-ресурсах, идентификационные (регистрационные) сведения, а также связи с периферийными устройствами и с географическим местоположением пользователя. Срок хранения данных варьируется в среднем от полутора месяцев – полугода до двух лет. Сохранение данных поставщиками услуг чаще осуществляется по приказу прокуратуры, нежели по судебному решению (в зависимости от необходимости получения доступа и от типа сведений). Обеспечение процесса извлечения данных может возлагаться как на компетентные правоохранительные органы или специализированные организации, так и на сотрудников юридического лица, подлежащего обыску (выемке).

11. Этика использования информационных технологий и стандарты контента являются одним из оснований классификаций киберпреступлений. Вместе с тем определение противоправного (также именуемого проблемным или деструктивным) контента в отдельных странах Глобального Юга не только небесспорно, но и вовсе отсутствует. Исходя из системного толкования и передовых практик арабских и азиатских стран (в частности ОАЭ, КСА, Республик Индия и Индонезия), подобное

регламентируется скорее компетентными органами в подзаконных актах и охватывает такие оценочные понятия, как уважение к ценностям общества, высшим интересам государства, религии, SARA, национальное единство, моральные принципы, безопасность государства, сохранение дружественных отношений (то есть принцип не навредить внешним сношениям), запрет слухов, дезинформации, разжигания розни, подстрекательства к совершению преступлений и нарушению правопорядка, нарушений прав интеллектуальной собственности, введения в заблуждение. Порядок ограничения доступа и удаления — чаще всего административный с возможностью обжалования в суде (в отдельных случаях — с привлечением гражданского общества). Отсутствие минимальных международных стандартов в данной области и отдельных каналов (механизмов) для взаимодействия затрудняет эффективное международное сотрудничество для оперативного пресечения правонарушений.

12. Несмотря на признание отдельными юрисдикциями виртуальных активов в качестве имущества для антиотмывочных, антикоррупционных и уголовно-процессуальных целей, фактически сохраняется общий порядок наложения обеспечительных мер, который может быть разделен на три модели: судебный (Республика Индонезия, ФДРЭ, КСА, ТР), внесудебный (Республика Индия, Катар) и смешанный (ОАЭ, Бахрейн, АРЕ) подходы. С учётом особых институциональных механизмов в рамках специальных административных районов и особых экономических (свободных финансовых) зонах предположим возможность оперативного реагирования, сбора и передачи информации о преступлении и расследования (производстве первоначальных следственных действий), которые способствуют оперативному наложению обеспечительных мер, включающих арест, замораживание и конфискацию.

Основным механизмом, применяемым при осуществлении международного сотрудничества в сфере уголовного судопроизводства, является взаимная правовая помощь по уголовным делам. Центральный орган, как и иные компетентные органы, могут различаться именно по характеру запросов по наложению ограничительных мер. Подробность регламентации процедур разнится даже в рамках одного региона.

13. Основной проблемой международного сотрудничества в борьбе с киберпреступностью (в целом) и уголовном судопроизводстве (в частности) является ограниченность существующих институциональных механизмов для Российской Федерации (ЛАГ, ОИС, ССАГПЗ, АС, IGAD и АСЕАН), неприсоединение ряда государств к международным договорам (например, в рамках ШОС) или их отсутствие (БРИКС). Активно развивается практика двусторонних форматов межгосударственного сотрудничества в виде совместных комитетов и комиссий в зарубежных странах, возможна проработка расширенных криминалистических учётов (банков электронных / цифровых следов) в рамках международных полицейских организаций и двусторонних контактов с соблюдением цифрового суверенитета государства и принципов трансграничной передачи данных, которые находятся ещё на стадии становления в рамках именно уголовного процесса. Последнее также способствовало бы выработке универсальных механизмов по блокировке неправомерного контента при наличии соответствующих международных стандартов.

14. Вследствие столь широкой повестки практически все государственные органы и многие представители частного сектора задействованы прямо или косвенно в сфере кибербезопасности, становясь субъектами или объектами воздействия. Проблемы должны рассматриваться не изолированно друг от друга, а в комплексе: наряду со своевременной криминализацией и пенализацией новых форм преступного использования ИКТ необходимо повышать квалификацию кадрового состава государственных (не только правоохранительных) органов, просвещать население через соответствующих амбассадоров или киберволонтёров в форме, доступной для различных уязвимых групп населения, формировать защищённые платформы с назначением ответственных для межведомственного взаимодействия, оперативной передачи информации и избежания дублирования (и, как следствия, бюрократического затягивания), а также расширять учёты и доступы правоохранительных органов к существующим информационным системам в государстве.

Сформулированные положения определяют ***теоретическую значимость проведенного исследования*** и позволяют выявить тесную взаимосвязь уголовно-правовых наук при противодействии киберпреступлениям и осуществлении международного сотрудничества в этой сфере. В работе теоретически обоснована необходимость:

- универсальных формулировок и учёта типологически новых видов при криминализации и пенализации киберпреступлений;

- новых юрисдикционных привязок для установления уголовной юрисдикции;

- активного разработки стратегических документов и развития профилактических мер;

- вовлечённости гражданского и научного сообщества, должностных лиц и органов смежных направлений в противодействие киберпреступлениям;

- урегулировании правового статуса и процессуального закрепления цифровых доказательств, а также криминалистического обеспечения расследования киберпреступлений с внедрением передовых практик;

- расширения понятия имущества, совершенствования механизма наложения обеспечительных мер на внутри- и межгосударственном уровнях;

- внедрения электронного документооборота (далее — ЭДО) и обеспечения трансграничной передачи данных для целей уголовного судопроизводства;

- регламентации содержания неправомерного контента и механизма ограничения доступа к нему и/или его удаления;

- совершенствования международно-правовых документов и налаживания двусторонних контактов.

Полученные результаты и сформулированные предложения по совершенствованию внутригосударственного регулирования и межгосударственного взаимодействия могут служить основной для дальнейших исследований в обозначенных областях.

Практическая значимость полученных результатов проведенного исследования видится в описании текущего состояния и оценке возможных изменений, необходимых для повышения эффективности деятельности

правоохранительных органов в международном сотрудничестве в сфере борьбы с киберпреступностью, а также выработке релевантных рекомендаций по совершенствованию национального законодательства и международно-правовых документов. Содержащиеся в исследовании выводы и предложения могут быть использованы в правотворческой деятельности, направленной на развитие и совершенствование внутригосударственного и международно-правового регулирования противодействия киберпреступлениям.

Апробация и внедрение результатов диссертационного исследования.

Диссертация подготовлена на кафедре уголовного права, уголовного процесса и криминалистики МГИМО МИД России, на заседаниях которой проходило её обсуждение.

Некоторые положения исследования были апробированы автором на следующих научных мероприятиях:

- VIII Международной научно-практической конференции «Уголовная политика и правоприменительная практика» (Санкт-Петербург, 30–31 октября 2020 года) с докладом на тему: «Современные угрозы правам человека со стороны киберпространства»;

- Международной научно-практической конференции преподавателей и аспирантов «Современное государство и правовая система» (Смоленск, 03 декабря 2020 года) с докладом на тему: «Проблемы противодействия преступлениям, совершаемым с использованием информационных технологий: российский и международный опыт»;

- XIV Международном круглом столе «Преступления в сфере экономики: российский и зарубежный опыт» (Москва, 03 ноября 2022 года) с докладом на тему: «Проблемы определения классификации экономических преступлений в ОАЭ»;

- XX Международной научно-практической конференции «Уголовное право: стратегия развития в XXI веке» (Москва, 19–20 января 2023 года) с докладом на тему: «Уголовно-правовая характеристика манипулирования рынком ценных бумаг и незаконного использования инсайдерской информации в ОАЭ»;

- II Международной научно-практической конференции «Актуальные вопросы обеспечения национальной безопасности» (Санкт-Петербург, 07 декабря 2023 года) с докладом на тему: «Риски отмывания (легализации) активов, полученных преступным путем, и финансирования терроризма в сфере гейминга»;

- круглом столе «Цифровые преступления: особенности квалификации» I Международного научно-практического форума «Право цифровой безопасности» (Москва, 24–25 апреля 2024 года) с докладом на тему: «Теоретико-правовая характеристика киберпреступлений в арабских странах»;

- сессии № 2 «Правовое регулирование в современном мире: традиционные инструменты и новые подходы» Молодёжного дня IX Юридического форума стран БРИКС (Москва, 18–21 сентября 2024 года) с докладом на тему: «Борьба с киберпреступлениями в странах Глобального юга на примере участников БРИКС и БРИКС+: сравнительно-правовые аспекты»;

- секции № 1 «Киберпреступность в Восточной Азии в эпоху региональных конфликтов» Международной научной конференции «Новое пространство международного сотрудничества» (Москва, 15 октября 2024 года) с докладом на тему: «Сравнительно-правовой анализ отдельных уголовно-процессуальных мер противодействия киберпреступлениям в странах Глобального юга на примере БРИКС и БРИКС+»;

- II Международной научно-практической конференции «Стратегии противодействия преступности в условиях изменяющейся реальности» (Кострома, 22 мая 2025 года): «Формы воздействия на преступность и их значение»;

- XXIII Международной научно-практической конференции «Уголовно-процессуальные и криминалистические чтения на Алтае» (Барнаул, 30 мая 2025 года) с докладом на тему: «Цифровые наркотики»;

- III Международной научно-практической конференции «Проблемы противодействия киберпреступности» (Москва, 4 июня 2025 года) с докладом на тему: «Особенности расследования киберпреступлений и доказывания: сравнительно-правовой анализ законодательства РФ и отдельных стран

Глобального Юга в контексте международного сотрудничества в сфере уголовного судопроизводства»;

- дискуссионной площадке «Цифровое будущее криминалистической науки» Международной научно-практической конференции «Криминалистические чтения на Байкале – 2025» (Иркутск, 20 июня 2025 года) с докладом на тему: «Криминалистические особенности фиксации и изъятия цифровых доказательств в отдельных странах Глобального Юга»;

- Академических слушаниях законов и законопроектов в сфере информационной безопасности МГИМО МИД России (11 апреля, 13 мая, 10 июля 2025 года).

По итогам ряда конференций были выпущены сборники, входящие в Российский индекс научного цитирования (РИНЦ), а по итогам третьей — подготовлена и опубликована научная статья: Цыплакова А.Д. Проблемы определения и классификации экономических преступлений в ОАЭ / В.А. Шестак, А.Д. Цыплакова // Уголовное право: стратегия развития в XXI веке. 2023. № 2. С. 273-281. Также переведенные материалы размещены в международном репозитории Social Science Research Network (SSRN).

Основные положения и выводы исследования отражены в подготовленных и опубликованных автором самостоятельно и в соавторстве научных статьях, 14 из которых – в научных журналах, включенных в Перечень рецензируемых научных изданий, в которых должны быть опубликованы основные научные результаты диссертаций на соискание ученой степени кандидата наук, на соискание ученой степени доктора наук Высшей аттестационной комиссии при Министерстве науки и высшего образования Российской Федерации по специальности 5.1.4. Уголовно-правовые науки:

1) Цыплакова А.Д. Проблемы регулирования уголовной юрисдикции в Королевстве Саудовская Аравия / В. А. Шестак, А.Д. Цыплакова // Мировой судья. — 2023. — № 2. — С. 2–6. DOI: 10.18572/2072-4252-2023-2-2-6;

2) Цыплакова А.Д. Международное полицейское сотрудничество: современная институциональная структура и тенденции развития / А. Г. Волеводз,

А.Д. Цыплакова // Международное уголовное право и международная юстиция. — 2023. — № 3. — С. 2–6. DOI 10.18572/2071-1190-2023-3-2-6;

3) Цыплакова А.Д. Понятие и сущность киберпреступлений в государствах-членах ССАГПЗ / В.А. Шестак, А.Д. Цыплакова // Мировой судья. — 2023. — № 4. — С. 2–7. DOI 10.18572/2072-4152-2023-4-2-7;

4) Цыплакова А.Д. Проблемы регулирования уголовной юрисдикции в Объединённых Арабских Эмиратах / В.А. Шестак, А.Д. Цыплакова // Российский следователь. — 2023. — № 7. — С. 65–68. DOI: 10.18572/1812-3783-2023-7-65-68;

5) Цыплакова А.Д. Уголовная ответственность юридических лиц в Объединенных Арабских Эмиратах / А.Г. Волеводз, А.Д. Цыплакова // Российский следователь. — 2023. — № 12. — С. 58–72. DOI: 10.18572/1812-3783-2023-12-58-62;

6) Цыплакова А.Д. Проблемы совершенствования прогнозирования преступности / В.А. Шестак, А.Д. Цыплакова // Расследование преступлений: проблемы и пути их решения. — 2023. — № 3 (41). — С. 78–84. DOI 10.54217/2411-1627.2023.41.3.008;

7) Цыплакова А.Д. Уголовная ответственность юридических лиц в Объединённых Арабских Эмиратах и Королевстве Саудовская Аравия: сравнение материальных и процессуальных аспектов / А.Г. Волеводз, А.Д. Цыплакова // Российский следователь. — 2024. — № 3. — С. 51–56. DOI: 10.18572/1812-3783-2024-3-51-56;

8) Цыплакова А.Д. Виктимологическая профилактика киберпреступлений в Королевстве Саудовская Аравия / В.А. Шестак, А.Д. Цыплакова // Мировой судья. — 2024. — № 4. — С. 2–7. DOI: 10.18572/2072-4152-2024-4-2-7;

9) Цыплакова А.Д. Цифровые доказательства в уголовном процессе государств-членов Совета сотрудничества арабских государств Персидского залива: правовой статус и процедуры признания / А.Г. Волеводз, А.Д. Цыплакова // Вестник экономической безопасности. — 2024. — № 2. — С. 21–29. DOI: 10.24412/2414-3995-2024-2-21-29;

10) Цыплакова А.Д. О некоторых особенностях получения цифровых доказательств в арабских странах на примере Объединенных Арабских Эмиратов и Королевства Бахрейн / А.Г. Волеводз, А.Д. Цыплакова // Российский следователь. — 2025. — № 1. — С. 45-49. DOI: 10.18572/1812-3783-2025-1-45-49;

11) Цыплакова А.Д. Борьба с киберпреступностью в странах Глобального Юга: сравнительно-правовое исследование / А.Д. Цыплакова // Пролог: журнал о праве. — 2025. — № 1. — С. 99–110. DOI: 10.21639/2313-6715.2025.1.10;

12) Цыплакова А.Д. Должностные лица и органы, обеспечивающие полноту судебной власти в арабских странах: понятие и полномочия / А.Д. Цыплакова // Вестник Дальневосточного юридического института МВД России имени И. Ф. Шилова. — 2025. — № 2. — С. 142-151;

13) Цыплакова А.Д. Международное сотрудничество в борьбе с киберпреступлениями: некоторые правовые проблемы в свете принятия Конвенции ООН против киберпреступности / А.Д. Цыплакова // Российский следователь. — 2025. — № 10.— С. 62-66;

14) Цыплакова А.Д. Противодействие киберпреступлениям в странах Глобального Юга: современное состояние, проблемы и перспективы / А.Д. Цыплакова // Право и управление. XXI век. — 2025. — № 3. — С. 62–75.

Ряд научных статей подготовлен и опубликован в изданиях, индексируемых в международных базах данных, в частности Scopus (4):

15) Tsyplakova A.D. Criminological features of the cybersecurity threats / V.A. Shestak, A.D. Tsyplakova // Law, State and Telecommunications Review. — 2023. — No. 15-2. — P. 187–203. DOI: 10.26512/lstr.v15i2.45997;

16) Tsyplakova A.D. Countering Cyberattacks on the Energy Sector in the Russian Federation and the USA / V.A. Shestak, A.D. Tsyplakova // BRICS Law Journal. — 2023. — Vol. 10. — No. 4. — P. 35–52. DOI:10.21684/2412-2343-2023-10-4-35-52;

17) Tsyplakova A.D. Classification of cybercrimes in GCC countries / V.A. Shestak, A.D. Tsyplakova // Law, State and Telecommunications Review. — 2024. — No. 16-1. — P. 65–78. DOI: 10.26512/lstr.v16i1.48885;

18) Tsyplakova A.D. Comprehensive approach to cybercrime prevention in Arab countries /A.D. Tsyplakova // Law, State and Telecommunications Review. — 2025. — No. 17-1. — P. 23–41. DOI: 10.26512/lstr.v17i1.53743.

Отдельные положения и результаты диссертационного исследования использованы при подготовке, написании и опубликовании в составе авторских коллективов работ:

- Collecting Electronic Evidence in Criminal Cases in Russia and Foreign Countries: Experiences and Problems: Monograph / editors S.P. Shcherba (Russian ed.) and P.A. Litvishko (English ed.). — Moscow: Publishing House “Gorodets”, 2024. — 224 p. — Chapter 1. The Concept and General Characteristics of Electronic Evidence in Criminal Proceedings (E.A. Arkhipova, E.V. Bykova, S.P. Shcherba, P.A. Smirnov, A.D. Tsyplakova and A.G. Volevodz). ISBN 978-5-907762-35-0;

- Противодействие криптовалютным преступлениям в зарубежных странах: учеб. пособие / В.Ф. Васюков, А.Г. Волеводз, К.К. Клевцов, Э.Л. Сидоренко, А.А. Титов, А.Д. Цыплакова / под ред. докт. юрид. наук, проф. А.Г. Волеводза. — М.: Юрлитинформ, 2025. — 504 с. ISBN 978-5-6053175-3-1.

Полученные в ходе диссертационного исследования результаты использовались в ходе проведения автором учебных занятий по дисциплинам «Уголовное право», «Криминология», «Ответственность за преступления в сфере высоких технологий», «Международные аспекты криминологии», «Международные аспекты борьбы с отмыванием денег и финансированием терроризма» со студентами бакалавриата и магистратуры Международно-правового факультета МГИМО МИД России (2024–2025 гг.) и слушателями курса повышения квалификации «Расследование киберпреступлений и преступлений в сфере высоких технологий» в Московской академии Следственного комитета имени А.Я. Сухарева (16 июня – 27 июня 2025 года), а также внедрены в учебный процесс кафедры информационных технологий и организации расследования киберпреступлений Факультета подготовки криминалистов Московской академии Следственного комитета имени А.Я. Сухарева по дисциплинам «Расследование киберпреступлений» и «Цифровые следы преступлений против личности» (2025 г.).

Структура диссертации, обусловленная целью и задачами исследования, включает введение, четыре главы (11 параграфов), заключение, приложения (8), список использованных источников и литературы (605). Выводы по главам содержатся в конце каждой из них. С учётом разнообразной терминологии составлен список используемых сокращений.

ГЛАВА I. УГОЛОВНО-ПРАВОВОЕ СОДЕРЖАНИЕ КИБЕРПРЕСТУПЛЕНИЙ В ОТДЕЛЬНЫХ СТРАНАХ ГЛОБАЛЬНОГО ЮГА

§ 1. Понятие и сущность киберпреступлений в отдельных странах Глобального Юга

Как на международном, так и на национальном уровнях понятийный аппарат имеет свою специфику ввиду лингвистических особенностей и охватываемого объёма уголовно-наказуемых деяний. Несмотря на распространённое использование термина «киберпреступления» в официальных переводах нормативных правовых актов на английский язык, а также в соответствующих соглашениях, в частности Конвенции о киберпреступлениях (Будапешт, 23.11.2001) (далее — Будапештская конвенция) [113] и Конвенции ООН против киберпреступности; Укрепление международного сотрудничества в борьбе с определёнными преступлениями, совершаемыми с использованием информационно-коммуникационных систем, и в обмене доказательствами в электронной форме, относящимися к серьёзным преступлениям (далее — Универсальная конвенция) [114], в аутентичных текстах можно найти различные наименования рассматриваемой категории преступлений на ряде языков (английском, французском, арабском, персидском, амхарском, китайском, индонезийском): электронные / компьютерные / сетевые / информационные преступления, преступления в сфере информатики / в сфере информационных технологий / в сфере информационных технологий и электронных транзакций, преступления, связанные с информационно-коммуникационными технологиями (системами) / с чувствительным оборудованием / автоматизированными системами обработки данных (далее — АСОД), киберпреступления, преступления против

---

[113] Convention on Cybercrime (Budapest, 23.XI.2001) // Council of Europe. URL: https://rm.coe.int/1680081561 (дата обращения: 09.03.2025).

[114] United Nations Convention against Cybercrime; Strengthening International Cooperation for Combating Certain Crimes Committed by Means of Information and Communications Technology Systems and for the Sharing of Evidence in Electronic Form of Serious Crimes // United Nations Treaty Collection. https://treaties.un.org/doc/Treaties/2024/12/20241224%2001-27%20PM/Ch_XVIII_16.pdf (дата обращения: 09.03.2025).

информатики и электроники, информационная преступность (см. Приложение № 1).

Киберпреступления выступают в качестве т.н. существительных общего рода, однако понятия встроены в рамки конкретной культуры, изучение лексикологии восточных языков, в том числе взаимоотношений между отдельными терминами и словами в пределах одного семантического поля, что представляется необходимым для общего понимания феномена[115].

В арабском и персидском языках применимы как транслитерация (араб. «الجرائم السيبرانية»; перс. «جرایم سایبری»), так и собственные обозначения, написание которых визуально сходно, поэтому требуется несколько грамматических отступлений и уточнений для уяснения содержания перечисленных в Приложении № 1 понятий: в арабском языке существует определённое и неопределённое состояния через артикль «ال» (аль-) — аналог «the» в английском языке[116]. В персидском языке подобное называется категорией выделенности, однако в учебниках, изданных в Иране, не сформулированы чёткие правила употребления артикля: «ای» ,«ئی» ,«یی» ,«ی».

При обозначении электронных преступлений (араб. «الجرائمُ الإلكترونيةُ») и информационных преступлений (араб. «الجرائمُ المعلوماتيةُ») существительное и прилагательное[117] стоят в одинаковых (определённых) состояниях в именительном падеже[118].

Преступления в сфере информатики (араб. «جرائمُ المعلوماتيةِ») и преступления в сфере информационных технологий (араб. «جرائمُ تقنيةِ المعلوماتِ») представляют собой идафы/идафатун[119], то есть «сопряженное состояние» через несогласуемые

---

[115] Балил ‘Абд ал-Карим. Терминология Корана: лингвистический и семантический анализ / пер. с англ. С. М. Коваленко. СПб.: Петербургское востоковедение, 2022. 216 с. С. 12–17.

[116] Рубинчик Ю.А. Грамматика современного персидского литературного языка / под ред. М.И. Карповой. М.: Восточная литература РАН, 2001. 600 с. С. 121.

[117] Оно может определяться по наличию характерного «ي» (йа), в то время как «ة» (та марбута или связанное т) указывает на женский род. Если речь идёт об неодушевлённом предмете во множественном числе, то прилагательное указывается по женскому роду. Тем не менее и существительные в единственном числе в женском роде имеют та марбута, поэтому нужно исходить из совокупности всех синтаксических и грамматических факторов.

[118] На что указывает огласовка «ُ» — дамма («у»)).

[119] С араб. «إضافة» — присоединение.

определения, выраженные именем существительным в родительном падеже[120] (может быть как в определённом, так и неопределённом состояниях). Тем не менее в таких случаях определяемое слово никогда не принимает артикль «аль-».

В персидском языке «аналогом» идафы[121] является изафетные словосочетания и определения, в которых используются имена существительные и которые состоят из главного и распространяющего членов. Именно эта ситуация и имеет место с компьютерными преступлениями (перс. «جرایم سایبری»).

Термин «ма'лююматун» (араб. «مَعْلُومَةٌ»)[122], как и «и'ыляямун» (араб. «إِعْلاَمٌ») переводится как информация, сведение[123]. Во множественном числе обозначается как «ма'лююмаатун» (араб. «مَعْلُومَاتٌ») и «и'ыляямаатун» (араб. «إِعْلاَمَاتٌ»)[124] — данные. В сочетании же с «такнийятун» (араб. «تَقْنِيَّةٌ» — техника) образуется устойчивое словосочетание с помощью идафы — информационные технологии (араб. «تقنية المعلومات»). Иногда понятие технологий транслитерируют с использованием арабской грамматики — «تكنولوجيات». Информационно-телекоммуникационные технологии же обозначаются как «тикнулюджиияту аль-ма'лююмаати ва-ль-итисоли» (араб. «تكنولوجيات المعلومات والاتصالات») или «тикнулюджиияту аль-и'ыляями ва-ль-итисоли» (араб. «تكنولوجيات الإعلام والإتصال»).

Китайское понятие «网络违法犯罪» / «網絡犯罪» можно разбить на три составляющих: «wǎngluò» (сеть или Интернет), «wéifǎ» (буквально нарушение закона / правонарушение или противоправный), «fànzuì» (буквально преступление / преступность или уголовный / преступный) — и содержит конструкцию, передающую отношения принадлежности и описания. Обычно для последнего используют служебную частицу «的» для показа неразрывной связи и передачи качественного признака, однако при едином термине её обычно опускают. Так,

---

[120] На что указывает огласовка «ِ» — кясра («и»).

[121] Как приводится в учебной и научной литературе, в Конституции Исламской Республики Иран более 60% текста — арабские слова почти в неизменном состоянии с морфологической точки зрения. Поскольку и фонетически, и семантически они органично вписываются, как грамматика, так и фонетика подверглась изменениям, а ряд терминов на фарси были вытеснены арабскими. Ibid. С. 77–78.

[122] На женский род единственное число указывает наличие «ة» — та марбута или связанное т.

[123] При переводе терминов с арабского языка используется словарь Х.К. Баранова.

[124] На множественное число указывает использование алифа с та «ات».

fànzuì выступает в качестве главного слова; *wéifǎ* используется для усиления и может опускаться, *wǎngluò* может расцениваться как зависимое прилагательное / существительное.

Примечательны и официальные переводы киберзаконов. Помимо англоязычных версий, которые подтверждают взаимозаменяемость многообразных терминов с киберпреступлениями, ещё одним доказательством служат аналоги на французском и португальском: регулирование Специального административного района Макао (КНР) официально переведено на португальский; Марокко, АНДР и Туниса — на французский. В то время в аутентичной версии указываются компьютерные преступления (кит. «電腦犯罪»), на португальском — дословно информационное преступление (порт. «à criminalidade informática»)[125]; «сетевая безопасность» или «безопасность Интернета» (кит. «網絡安全»), на португальском — кибербезопасность (порт. «cibersegurança») [126] . Схожая история с кибербезопасностью и киберпреступностью во франкоязычных версиях текстов законов стран аль-Магриба.

Наиболее часто встречаемыми являются преступления в сфере информационных технологий, примерами чего также могут служить Арабская конвенция о борьбе с преступлениями в области информационных технологий (Каир, 21.12.2010) (далее — Арабская конвенция)[127] и Эр-Риядский документ «Единообразное положение (модельный закон) о борьбе с преступлениями в области информационных технологий для стран Совета сотрудничества арабских государств Персидского залива» от 2013 г.[128].

---

[125] 第 11/2009 號法律. 編號. 2009. № 27. 版數. 971-978 [Закон № 11 о компьютерных преступлениях от 2009 года // Официальный Бюллетень. 2009. № 27. С. 971-978].

[126] 第 13/2019 號法律 // 公報. 2019. № 25. 版數 1884-1895 [Закон № 13 о сетевой безопасности от 2019 года // Бюллетень. 2019. № 25. С. 1884–1895].

[127] الاتفاقية العربية لمكافحة جرائم تقنية المعلومات [Арабская Конвенция о борьбе с преступлениями в области информационных технологий] // Лига арабских государств. URL: http://www.lasportal.org/ar/legalnetwork/Documents/2%التصديق20%على20%الاتفاقية20%العربية20%لمكافحة20%جرائم20%تقنية20%المعلومات0.pdf (дата обращения: 09.03.2025).

[128] وثيقة الرياض للنظام (القانون) الموحد لمكافحة جرائم تقنية المعلومات لدول مجلس التعاون لدول الخليج العربية [Эр-Риядский документ «Единообразное положение (модельный закон) о борьбе с преступлениями в области информационных технологий для стран Совета сотрудничества арабских государств Персидского залива»] // Электронная библиотека Совета сотрудничества арабских государств

Соглашение о сотрудничестве между правительствами государств-членов Шанхайской организации сотрудничества в борьбе с преступностью (Ташкент, 11.06.2010) [129] вводит понятие информационной преступности, под которой понимается использование информационных ресурсов и (или) воздействие на них в информационном пространстве в противоправных целях.

В глоссарии Национальной стратегии Государства Кувейт по кибербезопасности 2017–2020 гг., разработанной Управлением по регулированию коммуникаций и информационных технологий Государства Кувейт[130], термины «электронное преступление» и «киберпреступление» используются в качестве синонимов, хотя в Федеральном декрете-законе ОАЭ № 34 от 20.09.2021 «О борьбе со слухами и электронными преступлениями» (далее — ФДЗ ОАЭ № 34-2021)[131] «ас-сибраани» или «кибер» подразумевает «всё, что связано с компьютерными информационными сетями, Интернетом, различными информационными программами и всеми услугами, которые предоставляются в рамках перечисленного», в то время как «электронный» связан с различными видами технологий.

Наличие законодательного определения рассматриваемого вида деяний — это скорее тенденция регулирования в арабских странах, в особенности аль-Магриб. Положения Дахира[132] № 1-20-69 от 25.06.2020 «О принятии закона № 05-20 «О

Персидского залива URL: https://www.gcc-sg.org/ar-sa/CognitiveSources/DigitalLibrary/Lists/DigitalLibrary/1373542617/القانون%20والقضاء.pdf (дата обращения: 09.03.2025).

[129] Соглашение о сотрудничестве между правительствами государств-членов Шанхайской организации сотрудничества в борьбе с преступностью (Ташкент, 11.06.2010) // Шанхайская организация сотрудничества. URL: https://rus.sectsco.org/images/07e8/0c/05/1609696.pdf (дата обращения: 09.03.2025).

[130] الاستراتيجية الوطنية للأمن السيبراني لدولة الكويت ٢٠١٧-٢٠٢٠ [Национальная стратегия Государства Кувейт по кибербезопасности 2017–2020 гг.] // Управление по регулированию коммуникаций и информационных технологий Государства Кувейт. URL: https://citra.gov.kw/sites/ar/LegalReferences/Cyber%20Security.pdf (дата обращения: 09.03.2025).

[131] مرسوم بقانون اتحادي رقم ٣٤ لسنة ٢٠٢١ في شأن مكافحة الشائعات والجرائم الإلكترونية [Федеральный декрет-закон Объединённых Арабских Эмиратов № 34 2021 года «О борьбе со слухами и электронными преступлениями] // Официальная онлайн база законодательства ОАЭ. URL: https://uaelegislation.gov.ae/ar/legislations/1526 (дата обращения: 10.03.2025).

[132] Дахир / Захгирун (араб. «ظهير») — указ короля Марокко.

кибербезопасности» (далее — Дахир № 1-20-69)[133] повторяются в законопроекте ТР № 036/2024 «О кибербезопасности»[134]: киберпреступления — все действия, противоречащие национальному законодательству или международным договорам, ратифицированным Королевством Марокко, направленные на сети или информационные системы или выраженные в их использовании в качестве средства совершения проступка или преступления. В АНДР под преступлениями, связанными с информационно-телекоммуникационными технологиями, понимаются деяния, связанные с нарушением автоматизированной системы обработки данных (далее — АСОД), указанные в уголовном законе, и любые иные деяния, которые совершены или совершение которых облегчено с помощью ИТ или электронных средств связи в целом[135]. Примечательно, что криминализация в общеуголовном законе деяний, направленных против АСОД, характерна именно для стран аль-Магриб, в частности КМ[136].

Национальная стратегия Кувейта 2017–2020 гг. определяет киберпреступление как незаконное, неэтичное или несанкционированное (неуполномоченное) поведение и выход за рамки традиционной криминальной деятельности, которые совершаются через киберпространство посредством нетрадиционных методов для совершения обычных преступлений.

---

[133] ظهير شريف رقم ١.٢٠.٦٩ صادر في ٤ ذي الحجة ١٤٤١ (٢٥) يوليو بتنفيذ القانون رقم ٠٥.٢٠ المتعلق بالأمن السيبراني [Королевский указ № 1.20.69, изданный 04.12.1441, соответствующий 25.07.2020 «Об издании закона № 05.20 касающегося кибербезопасности»] // Официальный вестник. 2020. № 6904. С. 4160–4167.

[134] مقترح قانون عدد ٠٣٦/٢٠٢٤ يتعلق بالأمن السيبراني [Предлагаемый закон № 036/2024 о кибербезопасности] // Собрание народных представителей Тунисской Республики. URL: https://www.arp.tn/ar_SY/document/download/100242 (дата обращения: 09.03.2025).

[135] قانون رقم ٠٤-٠٩ مؤرخ في ١٤ شعبان عام ١٤٣٠ الموافق ٥ غشت سنة ٢٠٠٩، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها. [Закон № 04-09 от 14.08.1430, соответствующий 05.08.2009, включающий специальные правила по предупреждению и борьбе с преступлениями, связанными с информационно-коммуникационными технологиями] // Официальный вестник Алжирской Республики. 2009. № 47. С. 5–8.

[136] قانون رقم ٠٧.٠٣ بتتميم مجموعة القانون الجنائي في ما يتعلق بالجرائم المتعلقة بنظم المعالجة الآلية للمعطيات [Закон № 07.03, дополняющий свод уголовного закона в части преступлений, связанных с автоматизированными системами обработки данных] // Официальный вестник. 2003. № 5171. С. 4284–4285.

Под киберпреступлением (араб. «الجرائم السيبرانية») в Национальной стратегии кибербезопасности Государства Катар 2024–2030 г.[137] понимается неправомерное поведение или деяние, совершенное с использованием технологий.

Согласно Закону Государства Катар № 14 от 02.10.2014 «О борьбе с электронными преступлениями» (далее — Закон Катара № 14-2014), под электронным преступлением понимается любое действие, связанное с использованием средств информационных технологий, информационной системы или сети, незаконно, в нарушение положений закона[138]. Более лаконичная, но схожая формулировка содержится в Положении Королевства Саудовская Аравия от 27.03.2007 «О борьбе с преступлениями в сфере информатики» (далее — Положение КСА 2007 г.)[139] и в Законе Государства Кувейт № 63 от 07.07.2015 «О борьбе с преступлениями в сфере информационных технологий» (далее — Закон Кувейта № 63-2015)[140].

В Прокламации ФДРЭ № 958/2016 от 07.07.2016 «О компьютерных преступлениях» (далее — Прокламация ФДРЭ № 958/2016)[141] и Мнениях Верховного народного суда КНР, Высшей народной прокуратуры КНР, Министерства общественной безопасности КНР от 26.08.2022 «По некоторым вопросам применения уголовных процедур при разрешении дел о преступлениях в

---

[137] الإستراتيجية الوطنية الأمن السيبراني ٢٠٢٤-٢٠٣٠ دولة قطر [Национальная стратегия кибербезопасности 2024–2030 г. Государство Катар] // Национальное управление кибербезопасности Государства Катар. URL: https://ncsa.gov.qa/sites/default/files/2024-09/StrategyM9%20-%20AR%20OL_0.pdf?csrt=5654088632520333724 (дата обращения: 05.04.2025).

[138] قانون رقم ١٤ لسنة ٢٠١٤ بإصدار قانون مكافحة الجرائم الإلكترونية [Закон Государства Катар № 14 от 02.10.2014 «О борьбе с электронными преступлениями»] // Законодательства база Государства Катар «Al-Meezan». URL: https://www.almeezan.qa/LawPage.aspx?id=6366&language=ar (дата обращения: 09.03.2025).

[139] نظام مكافحة جرائم المعلوماتية ١٤٢٨ [Положение Королевства Саудовская Аравия от 27.03.2007 «Борьба с преступлениями в сфере информатики»] // Бюро экспертов Совета министров Королевства Саудовская Аравия. URL: https://laws.boe.gov.sa/BoeLaws/Laws/LawDetails/25df73d6-0f49-4dc5-b010-a9a700f2ec1d/1 (дата обращения: 09.03.2025).

[140] قانون رقم ٦٣ لسنة ٢٠١٥ في شأن مكافحة جرائم تقنية المعلومات [Закон Государства Кувейт № 63 2015 года «О борьбе с преступлениями в сфере информационных технологий»] // Электронное правительство Государства Кувейт. URL: https://www.e.gov.kw/sites/kgoarabic/Forms/CAITLawNo.63of2015oncombatingInformationTechnologyCrimes.pdf (дата обращения: 09.03.2025).

[141] Прокламация ФДРЭ № 958/2016 «О компьютерных преступлениях» // Федеральная газета Негарит. 2016. № 83. С. 9104–9131.

информационных сетях» (далее — Мнения КНР 2022 г.)[142] нет чёткого определения — перечислены лишь отдельные укрупнённые подвиды. При этом в национальной политике и стратегии кибербезопасности ФДРЭ 2021 г. [143] используется термин «киберпреступления» в значении деяний, совершенных с использованием информационно-телекоммуникационных сетей (далее — ИТС) и систем, в особенности Интернета. В уведомлении Высшей народной прокуратуры КНР от 22.01.2021 «Об издании положений касательно сетевых преступлений, расследуемых народной прокуратурой» (далее — уведомление ВНР КНР 2021 г.)[144] к ним относятся также посягательства, направленные против ИС, а равно связанные с этим.

В Рабочей программе по реализации Плана действий АСЕАН по борьбе с транснациональной преступностью (17.05.2002, Куала-Лумпур) отмечалось, что к кибер преступлениям (англ. «cyber crime») [145] относятся мошенничество с кредитными картами, отслеживание электронной почты (англ. «email tracing»), кибертерроризм, DDOS-атака, порча (англ. «defacing»), червь/вирусная атака[146].

Согласно Заявлению Регионального форума АСЕАН о сотрудничестве в борьбе с кибератаками и неправомерным использованием киберпространства террористами (28.07.2006, Кулуа-Лумпур), одним из киберпреступлений

---

[142] 关于办理信息网络犯罪案件适用刑事诉讼程序 [Мнения по некоторым вопросам применения уголовно-процессуальных норм при рассмотрении дел о преступлениях в информационных сетях] // Верховный народный суд КНР. URL: https://www.court.gov.cn/fabu-xiangqing-370301.html (дата обращения: 09.03.2025).

[143] The Federal Democratic Republic of Ethiopia. National Cyber Security Policy and Strategy. 2021 // INSA. URL: https://insa.gov.et/documents/20124/0/National+Cyber+security+Policy%26+StrategyFDRE.docx/03b2d42e-5cb3-f29e-f8f8-fe4ad3d94586?t=1639143692057&download=true (дата обращения: 25.03.2025).

[144] 最高检印发《人民检察院办理网络犯罪案件规定》 [Уведомление Высшей народной прокуратуры КНР «Об издании положений касательно сетевых преступлений, расследуемых народной прокуратурой»] // Высшая народная прокуратура КНР. URL: https://www.spp.gov.cn/spp/xwfbh/wsfbh/202101/t20210125_507446.shtml (дата обращения: 25.03.2025).

[145] Указано согласно тексту.

[146] Work Programme to Implement the ASEAN Plan of Action to Combat Transnational Crime Kuala Lumpur, 17 May 2002 // ASEAN. URL: https://asean.org/work-programme-to-implement-the-asean-plan-of-action-to-combat-transnational-crime-kuala-lumpur-17-may-2002/ (accessed 26.04.2025).

признавалось использование киберпространства в террористических целях (англ. «terroristic misuse of cyber crime»)[147] и использование ИТ в преступных целях[148].

При этом в Декларации (Рио де Жанейро, ФРБ, 07.07.2025) [149] киберпреступления выделяются в отдельную группу неправомерного использования информационно-коммуникационных технологий (далее — ИКТ) и искусственного интеллекта (далее — ИИ) наряду с мошенничеством, кибератаками и манипулированием данными.

Противозаконность на национальном или международном уровнях [150] как формальный признак преступления выступает в качестве основополагающего в дефинициях. Примером, помимо вышеперечисленного, служит и п. «ج» ст. 1 Указа Султана Омана № 12 от 06.02.2011 «О борьбе с преступлениями в сфере информационных технологий» (далее — Указ Султана Омана № 12-2011)[151].

При даче дефиниции законодатели фактически указывают, в качестве какого признака элемента состава преступления выступают ИТ, системы или сети. Как отмечает Главное управление по борьбе с коррупцией и по экономической и электронной безопасности Министерства внутренних дел Королевства Бахрейн, компьютер, сеть и лица, указанные в Законе Королевства Бахрейн № 60 от 30.09.2014 «О преступлениях в области информационных технологий» (далее —

---

147 Указано согласно тексту.

148 2006 ASEAN Regional forum statement on cooperation in fighting cyber attack and terrorist misuse of cyber space // CIL. URL: https://cil.nus.edu.sg/databasecil/2006-asean-regional-forum-statement-on-cooperation-in-fighting-cyber-attack-and-terrorist-misuse-of-cyber-space/ (accessed 27.04.2025).

149 Leaders' Declaration on Global Governance of Artificial Intelligence // BRICS. URL: https://brics.br/en/documents/presidency-documents/250706_brics_ggai_declarationfinal.pdf (accessed 07.07.2025).

150 В Прокламации ФДРЭ № 958/2016 в дефиниции в качестве компьютерного преступления указывается, в частности, конвенционное.

151 مرســـوم سلطاني رقـم ٢٠١١/١٢ بإصدار قانون مكافحة جرائم تقنية المعلومات [Указ Султана Омана № 12 2011 года «О борьбе с преступлениями в сфере информационных технологий»] // Министерство юстиции и правовым вопросам Султаната Оман. URL: https://mjla.gov.om/legislation/decrees/details.aspx?Id=213&type=L&lang=a (дата обращения: 09.03.2025).

Закон Бахрейна № 60-2014)[152], являются «источником», «целью»[153] или местом совершения преступления[154]. При этом термины «компьютер» и «компьютерная система» могут толковаться расширительно. В частности, в пояснительной записке к Прокламации ФДРЭ № 958/2016, указывается, что под ними понимаются любое устройство и инфраструктура[155], которые функционируют (получают и хранят данные) на основании компьютерной программы и без человека[156].

В юридической литературе можно найти узкие и широкие подходы к определению киберпреступлений, которые сводятся либо к получению выгоды с помощью систем, либо к подрыву их безопасности[157]. В отдельных случаях киберпреступления (араб. «الجرائم السيبرانية») сводятся лишь к компьютерным преступлениям (в сфере компьютерной информации) или скамы, не охватывая манипулирование идентификацией, нарушения конфиденциальности, распространение ложной информации и дезинформации, угроз суверенитету и культуре в киберпространстве[158]. Тем не менее подобный подход представляется нецелесообразным.

---

[152] قانون رقم ٦٠ لسنة ٢٠١٤ بشأن جرائم تقنية المعلومات [Закон Королевства Бахрейн № 60 от 30.09.2014 «О преступлениях в области информационных технологий»] // Комитет по законодательству и правовому мнению Королевства Бахрейн. URL: https://www.lloc.gov.bh/Legislation/HTM/K6014 (дата обращения: 10.03.2025).

[153] Исходя из отечественной уголовно-правовой мысли, речь скорее идёт об объекте, субъекте и средстве совершения преступления.

[154] مفهوم الجرائم الإلكترونية [Концепция электронных преступлений] // Главное управление по борьбе с коррупцией и по экономической и электронной безопасности Королевства Бахрейн. URL: https://www.acees.gov.bh/cyber-crime/the-concept-of-e-crimes/ (дата обращения: 09.03.2025).

[155] В пример приводят аппаратно-программное обеспечение, серверы, маршрутизаторы, устройства хранения данных, мобильные телефоны, телекоммуникационные системы, системы управления правительственной информацией по типу электронное здравоохранение и банкинг, налогообложение, СМИ, военная сфера и т.д.

[156] ማብራሪያ የኮምፒውተር ወንጀል አዋጅ [Разъяснение Закона о компьютерных преступлениях] // Законодательная база ФДРЭ. URL: https://www.lawethiopia.com/images/draft%20laws/Computer%20Crime%20-%20Explanatory%20note%20final%202.pdf (дата обращения: 10.03.2025).

[157] انوشا، سهیل، نیکجو، مهنوش، و کولیوند، روح اله. استراتژی امنیت سایبری. همایش ملی تحقیقات میان رشته ای در علوم مهندسی و مدیریت، ۱۴۰۰. [Сохаил Ануша, Махнуш Никджо, Рухолла Коливанда. Киберстратегия Ирана. Междисциплинарные исследования, инженерные и управленческие науки: третья конференция, Тегеран, 25.02.2022]. URL: https://sid.ir/paper/902054/fa (дата обращения: 05.04.2025); Patil H. B., Chowbe A. An Examination Of Digital Evidence And Its Relevance For Indian Forensic // Educational Administration: Theory and Practice. 2024. № 30(5). P. 6445-6452.

[158] Мохаммад Сулейман, Салах Газаль, Винсент Карчеди, Адель Аль-Адави. Метавселенная: возможности и проблемы безопасности. Эр-Рияд: Издательский дом университета Наифа, 2023.

Конституирующими признаками выступают средства или предметы посягательства: компьютеры, компьютерные / информационные / телекоммуникационные сети и системы, ИТ средства; информационные данные и информация, Интернет, электронные сайты, почты, учётные записи, документы и инструменты, средства платежа, записи, подписи, цифровые сертификаты, цифровая валюта и другие предметы преступного посягательства, а также незаконный контент, носящий оскорбительный, порочащий или аморальный характер. Нанесение ущерба перечисленному является либо целью, либо последствием. В качестве последнего в норме также могут быть указаны возбуждение вражды или ненависти (экстремистская направленность), а равно вред интересам личности, государства, монотеистическим религиям и закона[159].

При установлении уголовной ответственности за деяния рассматриваемого вида соответствующим понятием охватываются всевозможные посягательства, имеющие место в киберпространстве и связанные с ним: правонарушения регулирования телекоммуникационного сектора (лицензирование, оказание сертифицированных услуг, правила пользования социальными сетями, средствами связи и опубликования, в том числе электронной рекламы и контента), электронного документооборота в государственном и частном секторах, банковской системы (электронные средства платежа и виртуальные активы), защиты персональных данных, охраняемых законом тайн, а также чести и достоинства личности, документов цифровой идентификации (электронные подписи, печати и сертификаты), обеспечения безопасности объектов критической (информационной) инфраструктуры, прав интеллектуальной собственности и интересов потребителей. В отдельных случаях также выделяется регулирование труда (в части удалённой

محمد سليمان، صلاح غزال، فنسنت كارشيدي، عادل العدوي. الميتافيرس: الفرص والتحديات الأمنية. دار جامعة نايف للنشر، ٢٠٢٣. ١١٤ ص.]. C. 11, 68. 114 с. [

[159] Tsyplakova A.D. Classification of cybercrimes in GCC countries / V.A. Shestak, A.D. Tsyplakova // Law, State and Telecommunications Review. 2024. № 16-1. P. 65–78, Шестак В.А., Цыплакова А.Д. Понятие и сущность киберпреступлений в государствах-членах ССАГПЗ // Мировой судья. 2023. № 4. С. 2–7.

работы), государственной службы (использование социальных платформ, компетентных правоохранительных органов и вооруженных сил)[160].

С точки зрения правонарушений лицензированных видов деятельности отметим разность глубины проработки нормативно-правовой базы стран Глобального Юга. Например, согласно п. 16 ст. 6 Федерального декрета-закона ОАЭ № 50 от 03.10.2022 «О коммерческих сделках»[161] и Федеральному декрету-закону ОАЭ № 32 от 21.09.2021 «О коммерческих компаниях» [162], лицензированию подлежит экономическая деятельность, связанная с созданием, продажей, лизингом и управлением электронными платформами, веб-сайтами, интеллектуальными приложениями, данными и искусственным интеллектом и другими видами деятельности по цифровой трансформации. Совет министров ОАЭ уполномочен предоставлять временную лицензию на реализацию любого инновационного проекта, основанного на современных технологиях будущего характера или с использованием ИИ (Федеральный декрет-закон ОАЭ № 25 от 23.09.2018 «О проектах будущего» [163]). При этом под современными технологиями, согласно Федеральному декрету-закону ОАЭ № 14 от 04.09.2023 «Относительно торговли, которая основана на современных технологиях»[164], понимаются технологические платформы, используемые для современной торговли на основе технологий, будь то электронные, цифровые, биометрические, технологии искусственного

---

[160] Последнее отражено, например, в следующей работе: Rizal M., Yani Y.M. Cybersecurity Policy and Its Implementation in Indonesia // Journal of ASEAN Studies. 2016. № 4 (1). P. 61–78; نفيد ي. المكافحة التشريعية لبعض صور الجرائم المعلوماتية وأصناف المجرم المعلوماتي // المجلة العربية للدراسات الأمنية. ٢٠٢٢. ٣٨ (٢). ١٣٧-١٤٥ [Навид Ю. Законодательный контроль над некоторыми формами киберпреступности и типами киберпреступников // Арабский журнал исследований в области безопасности. 2022. № 38(2). С. 137-145].

[161] مرسوم بقانون اتحادي بإصدار قانون المعاملات التجارية [Федеральный декрет-закон о коммерческих сделках] // Законодательная база ОАЭ. URL: https://uaelegislation.gov.ae/ar/legislations/1610 (дата обращения: 29.09.2024).

[162] مرسوم بقانون اتحادي في شأن الشركات التجارية [Федеральный декрет-закон о коммерческих компаниях] // Законодательная база ОАЭ. URL: https://uaelegislation.gov.ae/ar/legislations/1542 (дата обращения: 29.09.2024).

[163] مرسوم بقانون اتحادي بشأن المشروعات ذات الصفة المستقبلية [Федеральный декрет-закон о будущих проектах] // Законодательная база ОАЭ. URL: https://uaelegislation.gov.ae/ar/legislations/1980 (дата обращения: 29.09.2024).

[164] مرسوم بقانون اتحادي في شأن التجارة من خلال وسائل التقنية الحديثة [Федеральный декрет-закон о торговле с помощью современных технологий] // Законодательная база ОАЭ. URL: https://uaelegislation.gov.ae/ar/legislations/2150 (дата обращения: 29.09.2024).

интеллекта, технологии Блокчейн или в технологических платформах, будь то доступ к веб-сайтам или доступ через интеллектуальные приложения.

В ряде государств Глобального Юга деятельность социальных платформ и сетей требует получение соответствующего вида лицензии или прохождение регистрации. Например, в КСА с 2022 г., в Катаре планируется с 2025 г. В Республике Индия, согласно подзаконным актам, в частности уведомлению от 11.04.2011 [165], кибер-кафе подлежат регистрации назначенным правительством компетентным органом. В отношении посредников в онлайн-играх и значимых социальных сетях (англ. «significant social media intermediaries and online gaming intermediaries»), дающих доступ к онлайн-играм, в которых пользователя кладут на депозит фиатные деньги или ожидают получения денежной выгоды (англ. «online real game»), согласно Информационно-технологическим правилам Республики Индия (Промежуточное руководство и Кодекс цифровых медиа) от 25.02.2021 (в ред. от 06.04.2023)[166] для контроля и надзора могут создаваться саморегулируемые органы.

Отметим, что государства при рассмотрении промежуточного проекта Универсальной конвенции взаимозаменяемо использовали термины «киберпреступления» (англ. «cybercrime») и «использование ИКТ в преступных целях» (англ. «use of information and communication technologies for criminal purposes»)[167]. Вдобавок предлагалось введение двух групп деяний, которые давно активно используются в юридической литературе различных исследователей

---

[165] Notification. New Dehli, 11.04.2011 // India Code: Digital Repository of Laws. URL: https://upload.indiacode.nic.in/showfile?actid=AC_CEN_45_76_00001_200021_1517807324077&type=rule&filename=Information%20TechnologyGuidelines%20for%20Cyber%20Cafe%20Rules)%20Rules,%202011%20.pdf (accessed 02.05.2025).

[166] The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 // India Code: Digital Repository of Laws. URL: https://upload.indiacode.nic.in/showfile?actid=AC_CEN_45_76_00001_200021_1517807324077&type=rule&filename=information_technology_(intermediary_guidelines_and_digital_media_ethics_code)_rules,_2021_(updated_06.04.2023)-.pdf (accessed 02.05.2025).

[167] A/AC.291/CRP.8/Rev.1 // UNODC. URL: https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Second_session/CRP8_Rev1.pdf (accessed 21.04.2025).

Глобального Юга [168] , а также в Руководстве Арабского университета наук безопасности им. принца Наифа бин Абдель Азиза 2024 г. [169]:

- преступления, совершаемые в киберпространстве (дословно с англ. «cyber-dependent crimes» — кибер-зависимые преступления), — противоправное поведение, для которого требуется использование компьютеров или компьютерных систем (включая хакерство, выкуп и кибервойну, но не ограничиваясь перечисленным);

- преступления с кибервозможностями (англ. «cyber-enabled crimes») — противоправное поведение, масштабы, охват или характер которого могут быть увеличены за счёт использования компьютеров или компьютерных систем (деяния против машин, с их использованием или в них).

Отдельного внимания заслуживают преступления в мета-вселенных [170] или мета-преступления (англ. «metaverse crimes»), в том числе кража цифровой личности (неправомерный доступ, риски токенизации), дипфэйки (угрозы с фальсифицированным материалом, обезличивание или имперсонализация, распространение заведомо ложных сведений), нарушение права на неприкосновенность цифровой частной жизни (отслеживание, агрессивное преследование, кибербуллинг), фишинг (кража учётных данных, неправомерный сбор персональных данных), цифровое мошенничество (схемы в сфере технической поддержки, инвестиций, обезличивания или имперсонализации),

---

[168] В отечественной науке также восприняты нижеуказанные термины. См., например, Захарцев С.И., Кийко А.Ю., Семенова И.В. Цифровая информация как квалифицирующий признак формирования частной методики расследования преступлений // Юридическая наука: история и современность. 2022. № 11. С. 126-134.

[169] عبدالرزاق المرجان ، محمد شوقي ، يوسف السبعاوي ، محمد المنشاوي ، سيوكي لي ، جلال الهاشل. الدليل الاسترشادي للتعامل مع الأدلة الجنائية الرقمية في الدول العربية. دار جامعة نايف للنشر، ٢٠٢٤. ٦٤ ص. [Аль-Марджан А.Р., Шаки М., Аль-Сабави Ю., Аль-Маншави М., Ли С., Аль-Хашель Дж. Руководство по работе с цифровыми судебно-медицинскими доказательствами в арабских странах. Издательский дом Университета Наиф, 2024. 64 с.].

[170] Точного определения нет. Предлагается понимать виртуальное пространство для социального взаимодействия между пользователями, имеющими цифровую копию себя, и купли-продажи виртуальных товаров и услуг. См. подробнее Cho J., Tom Dieck M.C., Jung T. What is the Metaverse? Challenges, Opportunities, Definition, and Future Research Directions. In Extended Reality and Metaverse - Immersive Technology in Times of Crisis / ed. M.C.Tom Dieck, T. Jung, S. Loureiro. Heidelberg: Springer, 2023.

виртуально-физические атаки, атаки с эффектом погружения в виртуальную реальность, виктимизация-суперреализм, неправомерное использование биометрических данных, деяния с использованием или против аватаров, виртуального имущества и активов (шантаж, вандализм, события, приводящие к сбоям), цифровые преступления сексуального характера (эксплуатация, насилие, харассмент), нарушения прав на интеллектуальную собственность[171].

Отметим, что большие языковые модели по типу «DeepSeek», «ChatGPT», «Microsoft Copilot» с использованием методов джейлбрейк могут использоваться в преступных целях, в частности написания основ кодов на языке программирования «C++» для клавиатурных шпионов (англ. «keylogger»), программ-вымогателей с последующей ручной корректировкой[172].

§ 2. Классификация и типология киберпреступлений в отдельных странах Глобального Юга

В качестве оснований для классификации киберпреступлений могут выступать законодательный, правоприменительный и доктринальный подходы. В части первого, правда, необходимо оговориться, что в ряде рассматриваемых государств в качестве источника права (законодательства)[173] выступает исламский шариат[174], хотя фактически решающую роль в его трактовке занимает уже именно

---

[171] El-Kady R. Unmasking Virtual Crimes: Investigating and Proving Evidence in the Metaverse. In Unveiling Social Dynamics and Community Interaction in the Metaverse. IGI Global, 2025. P. 389–444.

[172] Kovacs E. DeepSeek's Malware-Generation Capabilities Put to Test // Security Week. 13.03.2025. URL: https://www.securityweek.com/deepseeks-malware-generation-capabilities-put-to-test/ (accessed 12.06.2025); Maor E. AI Giving Rise of the 'Zero-Knowledge' Threat Actor // Security Week. 02.04.2025. URL: https://www.securityweek.com/ai-giving-rise-of-the-zero-knowledge-threat-actor/ (accessed 12.06.2025).

[173] В ст. 7 Конституции ОАЭ от 18.07.1971 (с поправками от 29.05.2023) и ст. 2 Конституции АРЕ от 19.01.2014 с поправками от 22.04.2019, ст. 4 Конституции ИРИ от 03.12.1979 (в ред. от 28.07.1989) и саудовском регулировании отправления правосудия и судебной власти указывается именно источник законодательства, а не права. См. подробнее: Shestak V.A., Tsyplakova A.D. Judge requirements and ethical issues in the Cooperation Council for the Arab States of the Gulf // Vestnik of Saint Petersburg University. Law. 2024. Vol. 15, No. 2. P. 493-507.

[174] Исламский шариат выступает в качестве источника регулирования взаимоотношения людей в целом и исполнения религиозных обязанностей. См. подробнее: Цыплакова А.Д. Некоторые юрислингвистические особенности источников уголовного права и уголовного процесса арабских государств // Право между Востоком и Западом. 2025. № 1. С. 28-38.

законодательная и судебная власти[175]. Вдобавок, в зависимости от принадлежности колоний (зависимых территорий) и, соответственно, влияния на кодификацию отдельных государств Глобального Юга [176] , необходимо руководствоваться общеуголовными и специализированными (не только кибер-) законами (королевскими указами).

Эмиратский законодатель установил самый широкий подход не только в наименовании, но и при охвате круга деяний: преступления в сфере информационных технологий и уголовно наказуемые правонарушения, совершаемые в сети Интернет (связанные с контентом, с распространением слухов и фэйковых новостей), образуют группу электронных преступлений. Более подробные законодательные виды одноимённых преступлений представлены в Законе Катара № 14-2014. Они охватывают частично экономические (подлог, электронное мошенничество, посягательства на права интеллектуальной собственности или связанные с электронными трансакциями), традиционные (посягательства на информационные системы, программное обеспечение) преступления и те, что имеют место в Интернете (направленные на контент, информационные сети и электронные сайты). К киберпреступлениям как к родовому понятию также следует отнести деяния, направленные против телекоммуникационной инфраструктуры или совершенные с её использованием, нарушения в сфере электронной торговли и собственно компьютерные преступления.

Исходя из нормативного регулирования в других арабских государствах, к преступлениям в сфере информационных технологий относятся:

- нападение на целостность и конфиденциальность информационных систем и систем данных; преступления, совершенные с использованием информационных

---

[175] Шариатские постулаты становятся юридически обязательными только после законодательного закрепления и государственного принятия в ряде арабских государств. См. подробнее: Сюкияйнен Л.Р. Особенности современного исламского права // Право между Востоком и Западом. 2025. № 2. С. 28–41.

[176] Об этом подробнее см., например, Трикоз Е.Н. Генезис и эволюция уголовно-правовой кодистики в традиции общего права: диссертация на соискание ученой степени доктора юридических наук / Трикоз Елена Николаевна. Москва, 2025. 503 с.

систем или данных; эксплуатация детей и физическое насилие; нарушение условий сбора электронных доказательств (ТР);

- атаки, направленные на безопасность информационных сетей, систем и технологии; преступления, совершаемые с использованием информационных систем (ИС) и ИТ; деяния, связанные с посягательством на неприкосновенность частной жизни, а равно совершенные администратором веб-сайта (АРЕ)[177];

- преступления, связанные с ИТ и данными; с ИТ-средствами; с контентом (КБ)[178];

- нарушение конфиденциальности, целостности и доступности электронных данных, информации и информационной системы; преступления, связанные с контентом; незаконное использование финансовой карты; злоупотребление ИТ-средствами; подлог и мошенничество в отношении информации (СО)[179].

Легальная классификация компьютерных преступлений, предусмотренная Законом ИРИ от 25.05.2009 «О компьютерных преступлениях» (далее — Закон ИРИ 2009 г.) [180] и Прокламацией ФДРЭ № 958/2016, в некоторой мере схожа, подразумевает открытый перечень и охватывает не только собственно компьютерные, но и иные киберпреступления:

- преступления против конфиденциальности данных, компьютерных и телекоммуникационных систем; против целостности и неприкосновенности данных, компьютерных и телекоммуникационных систем; кража и мошенничество,

---

[177] قانون مكافحة جرائم تقنية المعلومات رقم ١٧٥ لسنة ٢٠١٨ [Закон № 175 от 2018 года «О борьбе с преступлениями в сфере информационных технологий»] // Официальный вестник. 2018. № 32.2 (д). С. 3–25.

[178] قانون رقم ٦٠ لسنة ٢٠١٤ بشأن جرائم تقنية المعلومات [Закон Королевства Бахрейн № 60 от 30.09.2014 «О преступлениях в области информационных технологий»] // Комиссия по законодательству и юридическому заключению Королевства Бахрейн. URL: https://www.lloc.gov.bh/Legislation/HTM/K6014 (дата обращения: 09.03.2025).

[179] مرســـوم سلطاني رقـم ٢٠١١/١٢ بإصدار قانون مكافحة جرائم تقنية المعلومات [Указ Султана Омана № 12 2011 года «О борьбе с преступлениями в сфере информационных технологий»] // Министерство юстиции и правовым вопросам Султаната Оман. URL: https://mjla.gov.om/legislation/decrees/details.aspx?Id=213&type=L&lang=a (дата обращения: 09.03.2025).

[180] قانون جرائم رايانه ای [Закон о компьютерных преступлениях // Исследовательский центр Исламского совета ИРИ. URL: https://rc.majlis.ir/fa/law/show/135717 (дата обращения: 09.03.2025).

связанные с компьютерами; деяния против целомудрия и общественной морали; клевета и публикация ложных сведений, иные;

- преступления против компьютерной системы и компьютерных данных, деяния, связанные с подлогом, мошенничеством и кражей; нелегальный контент[181]; иные.

Однако в эфиопском законе также предлагается выделять и иные три категории деяний, исходя из определения компьютерного преступления: посягательство, направленное против компьютера, компьютерной системы, данных или сети; конвенционное деяние, совершенное с использованием компьютера, компьютерной системы, данных или сети; незаконные контент-данные, распространяемые посредством компьютера, компьютерной системы или сети.

Согласно Мнениям КНР 2022 г., к сетевым преступлениям относят случаи, угрожающие безопасности компьютерных информационных систем; случаи отказа от выполнения обязательств по управлению безопасностью информационных сетей, незаконного использования информационных сетей или оказания помощи в преступной деятельности в информационных сетях; случаи, когда информационные сети использовались для совершения основных преступлений, таких как мошенничество, азартные игры, нарушения в отношении персональных данных граждан. В уголовном же законе КНР[182] компьютерные преступления рассредоточены по кодексу: преступления против прав интеллектуальной собственности и преступления против социального управления и порядка[183]. В САР также разнится подход: в Гонконге деяния относятся к разделу «различные преступления» (кит. «杂 项 罪 行», англ. «Miscellaneous Offences») Закона от 19.11.1971 «О консолидации отдельных уголовных законов» (в ред. от

---

[181] Примечательно, что к этому виду относят преступления против общественной безопасности, которые в первоначальной редакции звучали как кибертерроризм. См. подробнее Yilma K.M. Some Remarks on Ethiopia's New Cybercrime Legislation // Mizan Law Review. 2016. № 10 (2). P. 448–458.

[182] 中华人民共和国刑法 [Уголовное право Китайской Народной Республики] // Национальный конгресс КНР. URL: http://www.npc.gov.cn/zgrdw/npc/lfzt/rlys/2008-08/21/content_1882895.htm (дата обращения: 06.06.2025).

[183] Цыплакова А.Д. Борьба с киберпреступностью в странах Глобального Юга: сравнительно-правовое исследование // Пролог: журнал о праве. 2025. № 1. С. 99–110.

23.03.2024) [184] , в Макао принят отдельный закон № 11 от 26.06.2009 «О компьютерных преступлениях» (в ред. 2020 г.)[185], криминализующий незаконные доступ к компьютерной системе, получение, использование или доступность компьютерных данных, перехват компьютерных данных, повреждение компьютерных данных, препятствование работе компьютерной системы, производство, импорт, экспорт, продажа, распространение или предоставление компьютерных устройств или данных, предназначенных для совершения преступлений, использование компьютерного устройства для имитации станции мобильной связи, незаконное раскрытие серьезной уязвимости компьютерной безопасности, компьютерные подлог и мошенничество.

Фактически в основу ложится то, в качестве какого признака выступает избранный компонент или всё устройство / система / сеть: предмета или средства преступного посягательства. В отдельных случаях криминализованные составы не имеют законодательного деления (см. Приложение № 3).

В арабской доктрине киберпреступления рассматривались в качестве подвида экономических преступлений [186] . Подобный подход был реализован в общеуголовном катарском законе[187]. Тем не менее *маалюн*[188] — лишь одно из

---

[184] 本条例旨在综合若干刑事成文法则 [Закон САР Гонконга от 19.11.1971 «О консолидации отдельных уголовных законов» (в ред. от 23.03.2024)] // Законодательная база Гонконга. URL: https://www.elegislation.gov.hk/hk/cap200!en-sc?INDEX_CS=N&xpid=ID_1438402821241_001 (дата обращения: 10.06.2025).

[185] 第 11/2009 號法律. 編號. 2009. № 27. 版數. 971-978 [Закон № 11 о компьютерных преступлениях от 2009 года // Официальный Бюллетень. 2009. № 27. С. 971-978].

[186] Imranuddin M. A Study of Cyber Laws in the United Arab Emirates: a thesis for the Master's Degree / Mohammed Imranuddin, Rochester Institute of Technology (Dubai Campus). New-York, 2017. P. 27; Masadeh A. M. S. Combating Cyber Crimes — Legislative Approach — A comparative Study (Qatar, UAE, UK) // Законодательная база Государства Катар «al-Meezan». URL: https://www.almeezan.qa/ReferenceFiles.aspx?id=54&type=doc&language=en (дата обращения: 09.03.2025). С. 16–17.

[187] قانون رقم ١١ لسنة ٢٠٠٤ بإصدار قانون العقوبات [Закон Государства Катар № 11 от 10.05.2004 «Наказания»] // Законодательства база Государства Катар «Al-Meezan». URL: https://www.almeezan.qa/LawPage.aspx?id=26&language=ar (дата обращения: 09.03.2025).

[188] Термин «маалюн» (араб. «مال») переводится как деньги, богатство, собственность, капитал или финансы в зависимости от контекста. См. подробней Шестак В.А., Цыплакова А.Д. Проблемы определения и классификации экономических преступлений в ОАЭ // Уголовное право: стратегия развития в XXI веке. 2023. № 2. С. 273-281; Цыплакова А.Д. Некоторые юрислингвистические особенности источников уголовного права и уголовного процесса арабских государств // Право между Востоком и Западом. 2025. № 1. С. 28–38.

охраняемых благ, на которое совершается посягательство при киберпреступлении. Помимо собственности объектом выступает физическое / юридическое лицо, государство (отдельные органы и в целом)[189]. Аналогичным образом три состава компьютерных преступлений были включены в главу 3 «преступления против прав собственности» эфиопского общеуголовного закона (ст. 706–709 Прокламации ФДРЭ № 414 от 09.05.2005 [190]). Приближенный подход отражен и в Законе Республики Индонезия № 1 от 02.01.2023 «Уголовный кодекс» (далее — Закон РИ № 1-2023) [191]: преступления против информатики и электроники включены в главу «Преступления, которые угрожают общественной безопасности людей, здоровью и имуществу».

Деяния, направленные против лица, нацелены на кражу личности или получение конфиденциальных данных с целью угроз и выполнения указаний злоумышленников, кибersталкинг (агрессивное преследование), преступления, связанные с порнографией; против государства — уничтожение данных и электронных файлов, ПО, подрыв деятельности, дестабилизация работы официальных сайтов и кража данных с целью угрозы безопасности страны, кибертерроризм, в частности хакерство, кибератаки, шпионаж, манипулирование данными, незаконная продажа предметов, оборот которых ограничен или запрещен, а также пропаганда, направленная на подрыв конституционного строя, распространение антиобщественной, аморальной или греховной деятельности либо провоцирующей насилие, хаос или конфликт среди населения.

---

[189] Этот подход основывается не только на мнении юристов, но и Национальной стратегии Кувейта 2018–2020 гг.
Alabdulatif A. Cybercrime and analysis of laws in Kingdome of Saudi Arabia: Science in Information System Security: a thesis for the Master's Degree / Afnan Alabdulatif; University of Houston. Houston, 2018. the Faculty of the Department of Information and Logistics Technology. P. 27–28, Amrutha A. ATT(H)ack-Anti-Cyber Crime Law in Saudi Arabia // STA Law Firm. 23.08.2017. URL: https://www.stalawfirm.com/en/blogs/view/atthack-anti-cyber-crime-law-in-saudi-arabia.html (дата обращения: 09.03.2025).

[190] Criminal Code of the Federal Democratic Republic of Ethiopia // Federal Negarit Gazeta, Proclamation No. 414/2004.

[191] Undang-undang (UU) Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana [Закон Республики Индонезия № 1 от 02.01.2023 «Уголовный кодекс»] // Законодательная база Республики Индонезия. URL: https://peraturan.bpk.go.id/Details/234935/uu-no-1-tahun-2023 (дата обращения: 10.02.2025).

С учётом специфики отдельных рассматриваемых государств, относящихся в том числе к религиозной правовой семье, ряд арабских правоведов подразделяют киберпреступления на академически определенные (несанкционированный доступ, выпуск контента, анализ трафика, изменение сообщения, отказ в обслуживании и маскарад) и определяемые нормами и ценностями общества: порнография, сексуальная эксплуатация и преступления, связанные с проституцией; незаконные финансовые и банковские операции, операции по кредитным картам; преступления против национальной безопасности и экономики; терроризм; вымогательство; нарушения конфиденциальности, запрет азартных игр[192], нарушения врачебной тайны[193], незаконный оборот и употребление наркотиков, незаконная торговля древностями, предметами старины, артефактами и произведениями искусства[194], людьми и оружием.

В более ранних арабоязычных исследованиях на основании ФЗ ОАЭ №2-2006 «О борьбе с преступлениями в сфере информационных технологий»[195] выделялись следующие категории: подстрекательство или пособничество в совершении грехов, связанных с проституцией, развратом, порнографическими материалами, наркотическими средствами и психотропными веществами; распространение слухов или информации, могущей нанести вред безопасности государства, его интересам или общественному порядку; облегчение совершения преступлений; посягательства, разжигающие вражду или ненависть; деяния, направленные против монотеистических религий[196].

---

[192] Первым данный запрет появился в КСА. См. подробнее Abu-taieh E., Alotaibi Sh., Aldehim Gh., Alfaries A. A. Cyber Security Crime and Punishment: Comparative Study of the Laws of Jordan, Kuwait, Qatar, Oman, and Saudi Arabia // International Journal of Cyber Warfare and Terrorism. 2018. № 8 (3). P. 46–59.

[193] Первым данным запрет появился в Кувейте. Ibid.

[194] Первым появился запрет в Султанате Оман. Ibid.

[195] قانون اتحادي رقم ٢ لسنة ٢٠٠٦ م في شأن مكافحة جرائم تقنية المعلومات [Федеральный закон Объединённых Арабских Эмиратов № 2 2006 года «О борьбе с преступлений в сфере информационных технологий»] // Официальная онлайн база законодательства ОАЭ. URL: https://elaws.moj.gov.ae/UAE-MOJ_OG/10002S_2006/01-31-2006_0442/UAE-OG_2006-01-30_00002_kait.pdf (дата обращения: 18.03.2025).

[196] Aissani R. The Ethics and Legislation of the New Media Use in the United Arab Emirates Analytical Study of the Law - Combating IT Crimes // AAU Journal of Business and Law. № 2 (1). 2020. P. 72–98.

Исходя из этики использования ИТ и стандартов медиаконтента, деяния могут быть направления против конфиденциальности и частной жизни, а также против ценностей общества[197]. При этом под запрещённым контентом[198] могут пониматься новости о ведущемся расследовании преступления или документ такого расследования, если следственный орган принял решение о его проведении в отсутствие тяжущихся сторон или запретил трансляцию любого из них в интересах общественного порядка, нравственности или установления истины; вопросы, касающиеся судопроизводства; новости о расследованиях или процедурах по делам об отцовстве, браке, опеке, разводе, алиментах и супружеской неверности; ход уголовных или гражданских дел, которые суды решили заслушать на закрытом заседании или воспрепятствовали их опубликованию; имена или фотографии подсудимых до вынесения окончательного решения по делу и без получения разрешения прокуратуры или компетентного суда, в зависимости от обстоятельств, в том числе в иностранных средствах массовой информации; имена или фотографии потерпевших от изнасилования и посягательства на честь.

Эмиратские правоприменители выделяют четыре вида киберпреступлений: деяния, совершенные против репутации и чести, против конфиденциальности и частной жизни, финансовые правонарушения и посягательства мошеннического характера[199].

Полицейские Гонконга подразделяют киберпреступления на неправомерный контент, связанный с детской порнографией, непристойными или порочащими материалами, неправомерный доступ к компьютерам через телекоммуникации, доступ к компьютеру с преступным или нечестным умыслом, уничтожение или повреждение имущества, при этом именуя их компьютерными[200]. Полицейские

---

[197] Aissani R. Anti-Cyber and information technology crimes laws and legislation in the GCC countries: A comparative analysis study of the laws of the UAE, Saudi Arabia and Kuwait / Rahima Aissani // Journal of Legal, Ethical and Regulatory Issues. № 25(1). 2022. P. 1–14.

[198] Содержание неправомерного, незаконного, деструктивного или запрещённого контента, а также порядок блокировки или ограничения доступа к нему рассматривается в § 2 главы II.

[199] Salem F., Fiscbach T. Указ. Соч. С. 4.

[200] 網絡安全及科技罪案 [Cyber Security and Technology Crimes] // Hong Kong Police Force. URL: https://www.police.gov.hk/ppp_tc/04_crime_matters/tcd/legislation.html (accessed 06.06.2025).

Макао — компьютерные мошенничества, кража услуг доступа в Интернет, онлайн-оскорбления других (например, на форумах), неправомерный доступ к устройствам (хакинг), шантаж, использование поддельной банковской карты и незаконное присвоение банковских сведений[201]. При этом их можно укрупнить в две группы: против морали и нравственности, а также в сфере экономики.

В то время как классификация предполагает сгруппирование деяний по определённым критериям, типология отвечает на вопрос, какие преступления наиболее распространены на конкретном уровне, исходя из изучаемой социальной среды: микросреды, среды среднего уровня, макросреды и мета-среды. В контексте рассматриваемых стран Глобального Юга и криминологии в международном измерении универсальный уровень (мета-среда) не представляется релевантным; макросредой выступает сам Глобальный Юг, который пока ещё не имеет чётко установленных границ ни в науке, ни на практике; среда же среднего уровня — регионы — и микросреды (государства) являются наиболее подходящими для исследования и последующего обобщения данных.

В 2010-х годах наиболее часто встречаемыми электронными инцидентами безопасности признавались хакинг компьютеров (компьютерных систем) и электронных аккаунтов конкретного лица, компании, кража личности, хакинг электронного сайта с помощью фэйков или искажения контента, вирусов и вредоносных программных обеспечений, посягательства на электронную почту (мошенничество, фишинг, спам, посягательства на честь и достоинство), вводящая в заблуждение реклама и трансляция неправомерного контента, подлог, мошеннические действия[202].

---

[201] 電腦 / 網絡犯罪 [Computer / Cybercrimes] // Polícia Judiciária do Governo da Região Administrativa Especial de Macau. URL: https://www.pj.gov.mo/Web//Policia/law/?lang=en (accessed 06.06.2025).

[202] Мишааль Абдулла бин Хусейн. تقرير مركز الإستجابة لطوارئ الحاسب الآلي لجرائم تقنية المعلومات ٢٠٠٨-٢٠٠٩ [Специальный Доклад Центра реагирования на компьютерные инциденты по преступлениям в области информационных технологий 2008-2009 гг.] // Официальная онлайн база законодательства ОАЭ. URL: https://elaws.moj.gov.ae/UAE-MOJ_Fokeh/15_العدد%20الرابع/UAE-MOJ_تقرير%20مركز%20الإستجابة%20لطوارئ%20الحاسب%20الآلي%20لجرائم%20تقنية%20المعلومات.html?val=UAE-FokehAA1 (дата обращения: 18.03.2025); Cyber Crime Investigation Manual. DSCI, 2011. 137 p. URL: https://jhpolice.gov.in/sites/default/files/documents-reports/jhpolice_cyber_crime_investigation_manual.pdf (accessed 08.04.2025), Shestak V.A.,

Это характерно для большинства изучаемых стран. В азиатском регионе, в частности Министерством обороны Индонезии, в 2013 г. выделялись следующие киберугрозы (в значительной мере кибератаки): перспективные постоянные угрозы (англ. «APT»), атаки типа «отказ в обслуживании» (англ. «DoS») и распределенные атаки типа «отказ в обслуживании» (англ. «DDoS»); атаки с целью порчи (англ. «defacement attacks»); атаки вредоносного ПО (англ. «malware attacks»); кибер-проникновения (англ. «cyber inflictions»); рассылка спама и фишинг (англ. «spamming and phishing»); злоупотребление протоколом связи — атака на спуфинг протокола управления передачей данных (англ. «abuse of Communication Protocol / a spoofing attack of Transmission Control Protocol»)[203].

Их также можно классифицировать как аппаратные и программные угрозы[204] (англ. «hardware and software threats»), а также угрозы для данных или информации (англ. «data/information threats»).

В арабоязычной литературе отмечается, что в 2012 г. в Королевстве Саудовская Аравия и Ливане наблюдалось активное распространение т.н. цифровых наркотиков (араб. «المخدرات الرقمية», англ. «digital drugs») [205] .

Tsyplakova A.D. Criminological features of the cybersecurity threats / V.A. Shestak, A.D. Tsyplakova // Law, State and Telecommunications Review. — 2023. — No. 15-2. — P. 187–203

[203] The Ministry of Defense of the Republic of Indonesia. A Road Map to Cyber Defense National Strategy. Jakarta: The Ministry of Defense of the Republic of Indonesia, 2013. P. 25.

[204] Иногда именуются также информационной коррупцией (англ. «Information Corruption»).

[205] Некоторые фармацевтические препараты оснащены проглатываемыми датчиками и передают сигнал с отметкой времени в приложение или другой внешний монитор изнутри желудка, предоставляя данные о соблюдении режима приёма лекарствам в режиме реального времени. См. подробнее Plowman R.S., Peters-Strickland T., Savage G.M. Digital medicines: clinical review on the safety of tablets with sensors // Expert Opin Drug Saf. 2018. №17. P. 849–52; Flore J. Ingestible sensors, data, and pharmaceuticals: subjectivity in the era of digital mental health // New Media Soc. 2021. № 23. P. 2034–2051; Won C., Kwon C., Park K., Seo J., Lee T. Electronic Drugs: Spatial and Temporal Medical Treatment of Human Diseases // Advanced Materials 2021. 2005930.

В литературе обозначается как электронный героин, цифровой героин, электронный кокаин, виртуальный наркотик, цифровая фармакея. См. подробнее Phillips T. “Electronic heroin”: China’s boot camps get tough on internet addicts // The Guardian. 28.08.2017. URL: http://www.theguardian.com/world/2017/aug/28/electronic-heroin-china-boot-camps-Internet-addicts (accessed 09.05.2025), Williams S. “Electronic heroin” spawns Chinese internet addiction camps // VOA. 25.08.2024. URL: https://www.voanews.com/a/electronic-heroin-spawns-chinese-Internet-addiction-camps/2427495.html (accessed 09.05.2025); Hadar A., Hadas I., Lazarovits A., Alyagon U., Eliraz D., Zangen A. Answering the missed call: Initial exploration of cognitive and electrophysiological changes associated with smartphone use and abuse // PLOS ONE. 2017. № 12(7). Article e0180094; Huddleston B. Digital cocaine: A journey toward iBalance. Christian Art Publishers, 2016; Kardaras N.

Национальному комитету по борьбе с наркотиками КСА, Генеральному управлению по борьбе с наркотиками КСА и Управлению по телекоммуникациям КСА было поручено не допустить попадания этих наркотиков к пользователям. Министр юстиции Ливанской Республики Ашраф Аль-Рифи, ранее занимавший пост директора службы безопасности в Бейруте, призывал заблокировать веб-сайты, продвигающие такую музыку. Доктор Сархан Аль-Муайни, заместитель директора Академии полицейских наук Шарджи, также призвал относиться к подобным записям как к галлюциногенным таблеткам[206]. Доктора Раги Аль-Омда, советник Медицинского комитета ООН, и Мухаммад Авида, профессор психиатрии Университета Аль-Азхар пояснили, что, несмотря на возможные терапевтические свойства (снижение боли, беспокойства и улучшение памяти), цифровые наркотики могут иметь негативные последствия[207].

Концепция заключается в использовании технологий для имитации эффектов от традиционных наркотических средств или психотропных веществ. Им может выступать приложение на смартфоне, особая музыка, и включать в себя симуляцию с помощью электродов или бинауральные ритмы, впервые обнаруженные Генри Уильямом Давом в 1839 г. и обозначенные как техника постукивания ушами, для вызова галлюцинаций сродни приёму ЛСД или экстази. Мощность звука составляет менее 1000-1500 Гц. Арабская организация информации и коммуникаций определяет их как звуковые волны в диапазоне от альфы до беты и дельты с разной частотой на каждое ухо (обычно с разницей в 10 Гц, не более 40 Гц)[208].

Glow kids: How screen addiction is hijacking our kids - and how to break the trance. St. Martin’s Griffin, 2017. 288 p.

[206] الهياس , خولة موسى , استغلال وسائل تقنية المعلومات في ارتكاب جرائم المخدرات وخاصة الرقمية : في ضوء قانون مكافحة جرائم تقنية المعلومات الاماراتي // مجلة العلوم الاقتصادية والإدارية والقانونية. ٢٠١٨. ٩. ٢. ١٦٨-١٨١ ص [Аль-Хайас, Хавла Мусса, Использование информационных технологий при совершении наркопреступлений, особенно цифровых: В свете закона ОАЭ о киберпреступности // Журнал экономических, административных и юридических наук. 2018. № 9(2). С. 168-181].

[207] ليلى ميسوم. المخدرات الرقمية: ظهور إدمان جديد عبر شبكة الإنترنت // مجلة جيل العلوم الإنسانية والاجتماعية. ٢٠١٢. ٢١. ١٦٣-١٧٤ ص [Лейла Мессум. Цифровые наркотики: Возникновение новой онлайн-зависимости // Журнал «Поколение гуманитарных и социальных наук». 2012. 21. С. 163-174].

[208] Fawzi M.M., Mansouri F.A. Awareness on Digital Drugs Abuse and its Applied Prevention Among Healthcare Practitioners in KSA // AJFSFM. 2017. № 1 (6). P. 625–633; McConnell P.A., Froeliger B., Garland E.L., Ives J.C., Sforzo G.A. Auditory driving of the autonomic nervous system: Listening to theta-frequency binaural beats post-exercise increases parasympathetic activation and sympathetic

Прослушивание в течение длительного времени может вызывать сонливость, головокружение, расслабление, эпилепсию, беспокойство, снижение концентрации и вялость [209] . Зависимость может проявляться как физиологически, так и психологически подобно употреблению психоактивных веществ: дрожание рук, расширенные зрачки, изменение в поведении. Зачастую она сопровождается зависимостью от связи (араб. «اضطراب إدمان الاتصال»), расстройством принудительного контакта (араб. «اضطراب الاتصال القهري») или гиперкоммуникативным синдромом (араб. «متلازمة الاتصال المفرط»)[210].

Как показывают тенденции 2020-х, наиболее типичными киберпреступлениями являются электронное пиратство, детская порнография, электронное преследование, кибератаки с помощью вирусов и вредоносного программного обеспечения и посягательства на финансовые карты, что свидетельствует о неизменности угроз со стороны киберпространства[211]. Особое место в азиатском регионе отводится мошенничествам, в том числе с использованием методов социальной инженерии, основанных на человеке или машине, а также электронному шантажу и фишингу [212] . Кибермошеннические операции проводятся под прикрытием промышленных объектов, технических парков, отелей и казино на территориях СЭЗ либо на приграничных территориях

---

withdrawal // Front Psychol. 2014. № 5:1248; Draganova R., Ross B., Wollbrink A., Pantev C. Cortical steady-state responses to central and peripheral auditory beats // Cereb cortex. 2007. № 18(5). P. 1193-1200.

[209] .عمر محمد بن يونس. المخدرات والمؤثرات العقلية عبر الإنترنت. الإسكندرية: دارالفكر الجامعى، ٢٠٠٤. ١٤٩ ص [Омар Мохаммед бин Юнис. Онлайн-наркотики и психотропные вещества. Александрия: Университетский дом аль-фикр, 2004. 149 с]; "أبو دوح خالد. المخدرات الرقمية: مقاربة للفهم. الندوة العلمية" المخدرات وتأثيرها على الشباب. الرياض: جامعة نايف العربية للعلوم الأمنية. ١٢-٢٠١٦.٠٢.١٨ [Абу Дух Х. Цифровые наркотики: Подход к пониманию. Научный симпозиум «Наркотики и их влияние на молодежь». Эр-Рияд: Наифский арабский университет наук безопасности. 12–18.02.2016].

[210] إناء فتيح على الرفاعي، خورج النسرين جورج عيسى زينة. المخدرات الرقمية" أنواعها والإدمان على مسببها. بيروت: المركز العربي للبحوث القانونية والقضائية، ٢٠٢٢. ١٢٨ ص [Хордж ан-Насрин Джордж Исса Зейна, Ваза Фатиха ибн аль-Рифаи. Цифровые наркотики, их виды и причины зависимости. Бейрут: Арабский центр правовых и судебных исследований, 2022. 128 с.].

[211] أنواع الجرائم الألكترونية [Типы электронных преступлений] // Главное управление по борьбе с коррупцией и по экономической и электронной безопасности Королевства Бахрейн. URL: https://www.acees.gov.bh/cyber-crime/types-of-cybercrime/ (дата обращения: 18.03.2025).

[212] Bara Pratama Mahaputra, Chairul Muriman, Surya Nita. Use Of Digital Forensic Technology To Reveal The Identity Of Social Engineering Crimes // Riwayat Educational Journal of History and Humanities. 2024. № 7 (3). P. 1000–1008; Khaled Eid. The Role of the Law in Protecting Individuals from Electronic Blackmail // Journal of Public Policy and Administration. 2024. № 8 (3). P. 103–108.

(насильно удерживаемыми гражданами азиатских государств) [213] . При этом сведения чаще приобретаются у поставщиков услуг, нежели используются схемы для получения персональных данных. Также используется ИИ для генерации текстов-скриптов, дипфэйков и клонирования голосов. По данным Управления по наркотикам и преступности Организации Объединённых Наций (далее — УНП ООН), мошенничество стало нацеливаться на китайскоязычные общины в регионе и во всем мире. Возглавляемые китайцами преступные операции стали набирать более разнообразный персонал, способный ориентироваться на более широкие «рынки». Группы же из других государств, включая Индонезию, Малайзию, Таиланд и Вьетнам, начали сотрудничать с китайскими партнёрами и позже создали свои собственные синдикаты. В пример можно привести сексуальное вымогательство (англ. «sextortion»), виртуальное похищение, особенно распространённое среди китайских студентов, обманная доставка (выявлено в САР КНР) и получение займов в социальных сетях у нелицензированных компаний (часто встречается в Индии). В 2023 году Индонезия депортировала 153 гражданина Китая, которые были задержаны в ходе рейдов по нескольким операциям, вымогавшим у жертв более 20 миллиардов индонезийских рупий (примерно 1,3 млн долларов США)[214].

В арабском регионе мошенничество связано с созданием подложных веб-сайтов, вводящей в заблуждение рекламы, использованием государственной символики, подложными вакансиями или трудоустройством через рекрутинговые сети, инвестициями, романтическими схемами и последующим шантажом, осуществлением купли-продажи фальшивых номеров для транспортного средства или недвижимости, а равно с резервом в известных ресторанах и отелях, в том

---

[213] UNODC. Casinos, Money Laundering, Underground Banking and Transnational Organized Crime in East and Southeast Asia, 2024. Global Fraud Summit. Tokyo: National Police Agency of Japan, 2024. 检察机关打击治理电信网络诈骗及其关联犯罪工 作 情 （2023 年）[Procuratorial Organs' Efforts to Combat and Govern Telecommunications Network Fraud and Related Crimes (2023)] // Supreme People's Procuratorate of the People's Republic of China. 30.11.2023. https://www.spp.gov.cn/xwfbh/wsfbt/202311/t20231130_635181.shtml#2 (accessed 11.05.2025).

[214] Transnational Organized Crime and the Convergence of Cyber-Enabled Fraud, Underground Banking and Technological Innovation in Southeast Asia: A Shifting Threat Landscape. Vienna: UNODC, 2024. P. 35, 39, 41, 48.

числе с помощью поддельных карт, выигранных лотерей, взломами мессенджеров (особенно WhatsApp)[215]. Ряд из перечисленных действий может быть лишь одним из этапов, а конечной целью выступает торговля людьми или сексуальная эксплуатация. При этом социальные сети по типу «Tagged» и «Facebook»[216], а также российские приложения для знакомств выступают в качестве инструмента вербовки[217].

В Азии же, особенно в КНР, мошеннические схемы, в частности афера с разделкой свиней (кит. «杀猪盘»), появившиеся ещё в 2010-х гг. и получившее широкое распространение в 2018 г., связаны с мессенджерами «WeChat», «QQ» и приложениями для знакомств «Soul», «Momo», «Tantan» [218] . Обычно кибермошеннические операции связаны с последующим отмыванием преступных активов — схемами по разделке свиней с использованием криптовалюты (англ.

---

[215] العنزي م. الجانب الموضوعي للاحتيال من خلال المواقع الإلكترونية في النظام السعودي مقارنًا بالقانونين المصري والكويتي // المجلة العربية للدراسات الأمنية. ٢٠٢٢. ٣٨ (١). ٠٤-١٧ ص.]Аль-Энези М. Содержательный аспект мошенничества с использованием веб-сайтов в саудовской системе по сравнению с египетским и кувейтским законодательством // Арабский журнал исследований в области безопасности. 2022. № 38 (1). С. 04–17]; سلطنة عُمان – 03/06/1445هـ الموافق 16/12/2023م - أهم أساليب الاحتيال الإلكتروني الحديثة [Султанат Омана 1445/06/03 АН соответствует 16/12/2023 г. н.э. - Наиболее важные методы современного электронного мошенничества.]. Аудиозапись: электронная // Совет арабских министров внутренних дел Лиги арабских государств. URL: https://www.aim-council.org/awareness-programs/cybercrime-videos/50276/ (дата обращения: 10.05.2025); - الإمارات [ОАЭ 02/02/1446هـ الموافق 06/08/2024 م - شرطة أبوظبي تحذر الجمهور من طرق وأساليب الاحتيال المتجددة 1446/02/02 АН соответствует 06/08/2024 AD - Полиция Абу-Даби предупреждает общественность о возобновляемых методах и методах мошенничества] // Совет арабских министров внутренних дел Лиги арабских государств. URL: https://www.aim-council.org/awareness-programs/cybercrime-posters/52783/ (дата обращения: 10.05.2025); 35% rise in cyber crimes in Q1 2025: ROP // Muscat Daily. 26.05.2025. URL: https://www.muscatdaily.com/2025/05/26/35-rise-in-cyber-fraud-crimes-in-q1-2025-rop/ (accessed 12.06.2025).

[216] Принадлежит компании «Meta», признанной экстремистской в РФ 21.03.2022 Тверским районным судом г. Москвы.

[217] سلطان الجمال، حميد البناي. مكافحة جرائم الاتجار بالبشر عبر شبكات التواصل الاجتماعي: دراسة استشرافية لسبل مكافحة الاتجار بالبشر من واقع قضايا الاتجار بالبشر بإمارة دبي. المكتب العربي للشؤون الأمنية والإعلامية العربية التابع لمجلس وزراء الداخلية العرب بجامعة الدول العربية، ٢٠٢١. ٤٠ ص.] Аль-Джамал С., Аль-Баннаи Х. Борьба с преступлениями, связанными с торговлей людьми, через социальные сети: перспективное исследование способов борьбы с торговлей людьми на основе случаев торговли людьми в эмирате Дубай. Арабское бюро по вопросам безопасности и СМИ Совета арабских министров внутреннил дел Лиги арабских государств, 2021. 40 с.]. URL: https://www.aimc-hr.org/mcms-store/pdf/886eddbd-7484-419c-a26d-e097f02e2a2c.pdf (дата обращения: 10.05.2025).

[218] Дамирчиев Э.И., Васюков В.Ф. Некоторые вопросы противодействия дистанционным мошенничествам в Китае // Научный вестник Орловского юридического института МВД России имени В.В. Лукьянова. 2024. № 2(99). С. 161-166.

«cryptocurrency-based pig butchering scams»). Каждый кошелек по пути накапливает средства от других жертв, перемещая их по кругу и последовательно через адреса посредников, впоследствии переводя в стейблкоины и циркулируя как через основные биржи, так и через нехостинговые кошельки. Средняя сумма составляет 26,8 млн долларов США. Особую озабоченность также вызывают онлайн-казино[219]. Также распространены обманные инвестиционные платформы по майнингу криптовалют (в частности, в Индии)[220].

Мошеннические схемы зачастую также связаны с нарушением законодательства о персональных данных. Например, в августе 2023 г. в КНР был вынесен приговор за следующую схему: приложение аккумулировало данные, которые предоставлялись трудоустроенными обманом сотрудниками и впоследствии перепродавались[221].

Отмечается мировая тенденция по расширению деятельности преступных групп, выходящая за рамки одного региона: азиатские синдикаты как лидеры в кибермошенничестве налаживают связи с картелями в Южной Америке, расширяют присутствие в Африке (особенно в Нигерии, Намибии, Анголе, Замбии) и используют Тихоокеанские острова для отмывания активов, полученных преступным путём. Основной площадкой для взаимодействия выступают мессенджеры «Telegram» и «Huione Guarantee»[222].

---

[219] Pig Butchering Scams: What the Data Shows // TRM Labs. 02.2023. URL: https://www.trmlabs.com/post/pig-butchering-scams-what-the-data-shows (accessed 11.05.2025); Crypto Crime Mid-Year Update // Chainalysis. 08.2024. URL: https://www.chainalysis.com/blog/2024-crypto-crime-mid-year-update-part-2/ (accessed 04.05.2025).

[220] Васюков В.Ф., Стражинская А.Н. Об оперативно-розыскных и следственных мерах противодействия легализации преступных доходов с использованием криптовалют // Российское право: образование, практика, наука. 2024. № 4. С. 68-78.

[221] 个人信息保护写进快板书 [Защита персональных данных записана в книге с хлопушкой] // Газета «People Daily». 01.11.2024. URL: http://society.people.com.cn/n1/2024/1101/c1008-40351843.html (дата обращения: 06.06.2025).

[222] Недавно переименовались в «Haowang Guarantee», дистанцируясь от «Huione Group», будучи дочерней компанией. Расположена в Камбодже, однако имеет связи с Канадой, Польшей, США, Гонконгом и Сингапуром. См. подробнее Inflection Point: Global Implications of Scam Centres, Underground Banking and Illicit Online Marketplaces in Southeast Asia. UNODC, 2025. 85 p. P. 3–11.

Арабская стратегия по кибербезопасности 2023–2027 гг.[223], разработанная Арабской организацией ИКТ и утверждённая 24.01.2024, выделяет ненадёжность паролей, фишинговые атаки и социальную инженерию как главные проблемы. Уязвимости в ПО часто используются при совершении кибератак, в том числе политически мотивированных. Таким образом, например, было похищено более 54 тыс. электронных файлов со сведениями о более чем 2 млн граждан Марокко из Национального агентства социального страхования и Министерства труда Марокко с последующим размещением в одном из открытых каналов мессенджера «Telegram» и Даркнете[224]. При этом отдельное внимание уделяется дезинформации и слухам. Появилось понятие электронных мух (араб. «الذباب الإلكترون») — армии фэйковых аккаунтов, управляемые Интернет-ботами, для распространения конкретного неправомерного или проблемного контента[225].

Согласно исследованиям, в странах АСЕАН в 2020 году в качестве киберугроз среди прочего выделялись компрометация деловой электронной почты, перехват данных в электронной коммерции, вредоносное ПО как услуга (англ. «Crimeware-as-a-Service»), криптоджекинг[226].

В Политике по расширению прав и безопасности детей в Интернете Африканского союза (21.05.2024)[227] в качестве угроз выделяются кибер-агрессия, кибер-буллинг, распространение материалов о сексуальном насилии в отношении

---

[223] Arab Cybersecurity Strategy 2023–2027 // Ministry of technologies and communications of Tunis. URL: https://www.mtc.gov.tn/fileadmin/user_upload/Arab_Cybersecurity_Strategy_2023-2027_White_Paper.pdf (accessed 05.05.2025).

[224] Ответственность за кибератаку взяла на себя алжирская группировка «JabaROOT», указавшая на месть за атаки на алжирские Интернет-ресурсы как мотив. Morocco investigates major data breach allegedly by Algerian hackers // The Record. 11.04.2025. URL: https://therecord.media/morocco-investigates-breach-hackers-algeria (accessed 12.06.2025).

[225] قانصو علي. الحرب الإلكترونية // مجلة الدفاع الوطني البناني. ٢٠٢١. ١١٨. ٣-٣٥ ص [Кансо Али. Электронная война // Журнал национальной обороны Ливана. 2021. № 118. С. 3–35].

[226] Estiyovionita K., Sitamala A. ASEAN’s role in cybersecurity maintenance and security strategy through an international security approach // LaJiL. 2022. № 4 (2). P. 79-86.

[227] African Union Child Online Safety and Empowerment Policy // African Union. URL: https://au.int/sites/default/files/documents/43798-doc-African_Union_Child_Online_Safety_and_Empowerment_Policy_Feb_2024.pdf (accessed 04.05.2025).

детей, сексуальная эксплуатация детей, которые в значительной мере охвачены международными договорами (см. Приложение № 4).

Отдельного внимания заслуживает феномен кибертерроризма[228], который пока нашёл отражение не во всех международных документах и трактуется двойственно: использование ИКТ в террористических целях и посягательства на объекты критически важной инфраструктуры (КИИ) в целях дестабилизации. При этом ИИ может использоваться для генерации дипфэйков[229], обхода систем безопасности и автоматизации кибератак. Особую озабоченность по этому поводу в официальных позициях выражает Китай[230].

§ 3. Особенности криминализации киберпреступлений в отдельных странах Глобального Юга

В качестве особенностей криминализации и пенализации посягательств в рассматриваемых странах Глобального Юга отметим следующее: многообразие нормативных актов, на которые оказали влияние в том числе различные международные договоры на региональном уровне, разные подходы к элементам составов преступлений, субъектам, подлежащим ответственности, применимых наказаний, сочетание начал уголовной и административной ответственности, а также юрисдикционные принципы, отягчающие обстоятельства и основания для освобождения от ответственности (наказания).

Присоединение к соответствующим международным документам и их ратификация предопределяет уголовно-правовую политику государства. Так,

---

[228] Барака А. Цифровой терроризм: как современные технологии способствуют росту экстремизма и финансированию терроризма // Финансовая безопасность. 2025. № 4. С. 67–69.

[229] Данная проблематика проявляется и в генерации неправомерного контента в целом. Об этом см. Бессонов А. А. Искусственный интеллект как орудие преступлений и средство их расследования // Государственная научно-техническая политика в сфере криминалистического обеспечения правоохранительной деятельности: сборник научных статей по материалам международной научно-практической конференции, Москва, 26 мая 2023 года / Академия управления МВД России. Том Часть 1. Москва: Академия управления Министерства внутренних дел Российской Федерации, 2023. С. 10-17.

[230] 中国关于网络空间国际规则的立场 [Позиция Китая по международным правилам киберпространства] // МИД КНР. 2021. URL: https://www.mfa.gov.cn/wjb_673085/zzjg_673183/jks_674633/zclc_674645/qt_674659/202110/t20211012_9552671.shtml (дата обращения: 07.07.2025).

Будапештская конвенция подписана и ратифицирована двумя государствами из рассматриваемого круга стран Глобального Юга: Марокко (29.06.2018 / 01.10.2018) и Тунисом (08.03.2024 / 01.07.2024), что, по мнению некоторых исследователей, восполняет существующие правовые пробелы[231].

Арабская Конвенция же подписана 18 государствами, однако КСА до сих пор не ратифицировало её[232]. Зачастую к ней нет прямых отсылок в законодательстве[233]. Исключением среди ССАГПЗ является Декрет-закон Королевства Бахрейн № 54 29.11.2018 «Об электронных коммуникациях и сделках» [234] . Некоторые исследователи отмечают отсутствие практической применимости указанного документа[235].

Несмотря на то, что КМ, КБ, АНДР, АРЕ и ТР являются государствами-членами Африканского союза, по состоянию на 08.07.2024 только Тунис является подписантом Конвенции АС о кибербезопасности и защите персональных данных (Аддис-Абеба, 27.06.2014)[236] с 23.04.2019[237].

К ШОС присоединились ИРИ и Республика Индия, а партнёрами по диалогу выступают Бахрейн, Египет, Катар, Кувейт, ОАЭ и КСА, однако они не присоединились к Соглашению между правительствами государств-членов

---

[231] Maleh Ya., Maleh Yo. The Moroccan View on Cybersecurity In Cybersecurity in Morocco / ed. by Ya. Maleh, Yo. Maleh. Springer Cham, 2022. P. 41–50.

[232] التصديق على الاتفاقيه العربية لمكافحة جرائم تقنية المعلومات [Ратификация Арабской конвенции о борьбе с преступлениями в области информационных технологий] // Лига арабских государств. URL: http://www.leagueofarabstates.net/ar/legalnetwork/Documents/20%العربية%20الاتفاقيه%20على%20التصديق%20المعلومات%20تقنية%20جرائم%20لمكافحة%20.pdf (дата обращения: 09.03.2025).

[233] Hakmeh J. Cybercrime and the Digital Economy in the GCC Countries / J. Hakmeh. London: Chatham House, 2017. P. 12.

[234] مرسوم بقانون رقم ٥٤ لسنة ٢٠١٨ بإصدار قانون الخطابات والمعاملات الإلكترونية [Декрет-закон Королевства Бахрейн № 54 2018 года «Об электронных коммуникациях и сделках»] // Электронная база законодательства Королевства Бахрейн. URL: https://www.legalaffairs.gov.bh/HTM/L5418.htm (дата обращения: 09.03.2025).

[235] Hakmeh J. Указ. Соч. Там же.

[236] African Union Convention on cyber security and personal data protection // African Union. URL: https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf (дата обращения: 09.03.2025).

[237] Status List // African Union. URL: https://au.int/sites/default/files/treaties/29560-sl-AFRICAN_UNION_CONVENTION_ON_CYBER_SECURITY_AND_PERSONAL_DATA_PROTECTION.pdf (дата обращения: 09.03.2025).

Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности (Екатеринбург, 16.06.2009)[238].

Перечисленные факты свидетельствуют о тенденции неприсоединения к международным договорам с целью сохранения собственного подхода к криминализации и пенализации деяний. Вдобавок в ряде случаев считается, что рассматриваемые конвенции (соглашения) по охвату преступлений отличаются незначительно (см. Приложение № 4).

С точки зрения национальных правовых регуляторов отметим разнообразие нормативно-правовой базы, включающей как общеуголовное, так и специализированное, а равно и неуголовно-правовое регулирование [239] ввиду смешанности правовых систем[240], юридико-технических и юрислингвистических особенностей. На первое указывалось ещё в Модельном эмиратском арабском законе «О борьбе с преступлениями в сфере информационных технологий и подобными», утверждённом резолюцией Совета министров юстиции арабских стран (ЛАГ) № 495-91д от 10.08.2003 и Советом министров внутренних дел арабских стран (ЛАГ) № 417-21д от 2004 г.[241].

Так, использование ряда конструкций расширяет применимость традиционных законов, напрямую не затрагивающих кибербезопасность. Во-

---

[238] Соглашение между правительствами государств-членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности (Екатеринбург, 16.06.2009) // Шанхайская организация сотрудничества. URL: https://rus.sectsco.org/20090616/1609633.html (дата обращения: 09.03.2025).

[239] Ряд применимых актов отражены в Приложении № 2.

[240] В последнее время разделение государств по чётким критериям классической триады правовых семей представляется нецелесообразным. Страны Глобального Юга не являются представителями исключительно одной традиции.

[241] قانون الإمارات العربي الاسترشادي لمكافحة جرائم تقنية المعلومات [Модельном эмиратском арабском законе о борьбе с преступлениями в сфере информационных технологий] // Арабская юридическая сеть ЛАГ. URL: http://www.leagueofarabstates.net/ar/legalnetwork/PublishingImages/Lists/TypicalArabLaws/AllItems/11.%20%D9%82%D8%A7%D9%86%D9%88%D9%86%20%D8%A7%D9%84%D8%A5%D9%85%D8%A7%D8%B1%D8%A7%D8%AA%20%D8%A7%D9%84%D8%B9%D8%B1%D8%A8%D9%8A%20%D8%A7%D9%84%D8%A7%D8%B3%D8%AA%D8%B1%D8%B4%D8%A7%D8%AF%D9%8A%20%D9%84%D9%85%D9%83%D8%A7%D9%81%D8%AD%D8%A9%20%D8%AC%D8%B1%D8%A7%D8%A6%D9%85%20%D8%AA%D9%82%D9%86%D9%8A%D8%A9%20%D8%A7%D9%84%D9%85%D8%B9%D9%84%D9%88%D9%85%D8%A7%D8%AA.pdf (дата обращения: 07.04.2025) (на араб. яз.).

первых, публикация каких-либо сведений, изображений, записей, аудио- или видеоматериалов или совершение действия «*любым иным способом*» может охватывать и использование технических средств связи, электронно-вычислительные машины (ЭВМ) и ИТС «Интернет». Например, ст. 6.2 Федерального закона ОАЭ № 51 от 09.11.2006 «О борьбе с преступлениями, связанными с торговлей людьми» (в ред. ФЗ № 1 от 15.01.2015)[242]: «*любому лицу, которое публикует любым способом имена или фотографии жертв или свидетелей, причастных к преступлениям, связанным с торговлей людьми, назначается лишение свободы и/или штраф в размере не менее десяти тысяч дирхамов ОАЭ».* «*Любой, кто поощряет других лиц устно, письменно или любым иным способом совершать какие-либо действия, которые считаются незаконными в соответствии со статьей 159 настоящего Закона[243], наказывается лишением свободы на срок не более двух лет*» (ст. 161 Закона ИХК № 16 от 04.10.1960 «О преступлениях» в ред. Закона № 10 2022 г.[244]). Схожие примеры можно найти и в ст. ст. 224, 467 Закона ИХК № 16 от 04.10.1960 «О преступлениях», ст. ст. 196, 217, 373 ФДЗ ОАЭ № 31 от 20.09.2021 «Преступления и наказания»[245], ст. 44 Положения КСА от 03.04.2012 «О борьбе с террористическими преступлениями и его финансированием»[246]).

---

[242] قانون اتحادي رقم ٥١ صادر بتاريخ ٢٠٠٦/١١/٠٩ م في شأن مكافحة جرائم الاتجار بالبشر [Федеральный закон ОАЭ № 51 от 09.11.2006 «О борьбе с преступлениями, связанными с торговлей людьми» (в ред. ФЗ № 1 от 15.01.2015)] // Официальная онлайн база законодательства ОАЭ. URL: https://elaws.moj.gov.ae/UAE-MOJ_OG/10002S_2006/11-14-2006_0457/UAE-OG_2006-11-09_00051_kait.pdf (дата обращения: 18.03.2025).

[243] *Незаконное объединение подстрекает или поощряет пропаганду следующих действий:*
а) отмена конституции Королевства революцией или саботажем;
б) свержение существующего правительства в Королевстве согласно Конституции с помощью силы и насилия;
в) саботировать или нанести ущерб средствам иорданского правительства в Королевстве.

[244] قانون العقوبات رقم ١٦ لسنة ١٩٦٠م مقام [Закон № 16 «О преступлениях» 1960 г.] // Министерство юстиции Иорданского Хашимитского Королевства. URL: https://www.moj.gov.jo/ebv4.0/root_storage/ar/eb_list_page/1960_لسنة_16_رقم_قانون_العقوبات_وتعديلاته.pdf (дата обращения: 25.03.2025).

[245] مرسوم بقانون اتحادي رقم ٣١ لسنة ٢٠٢١ بإصدار قانون الجرائم والعقوبات [Федеральный декрет-закон Объединённых Арабских Эмиратов № 31 от 20.09.2021 «Преступления и наказания»] // Официальный сайт Комитета министров ОАЭ. URL: https://laws.uaecabinet.ae/ar/materials/law/1529?page=1 (дата обращения: 25.03.2025).

[246] نظام مكافحة جرائم الإرهاب وتمويله [Положение «О борьбе с террористическими преступлениями и его финансированием»] // Бюро экспертов Совета министров Королевства Саудовская Аравия. URL:

Во-вторых, формулировки «*любое нарушение настоящего закона (положения) наказывается…*» в актах, затрагивающих правовой статус или применение ИТ/ИС (см. Приложение № 2), расширяют возможный перечень киберпреступлений. Однако в некоторых работах исследователей из стран Глобального Юга киберрегулирование рассматривается отдельно от электронной коммерции, телекоммуникаций, неприкосновенности частной жизни в сетях и СМИ [247]. Вдобавок, с учётом государственного устройства и выделения свободных финансовых (экономических) зон, регулирование может охватывать и федеральный, и региональный уровни. Ярким представителем подобного является ОАЭ и, в частности, эмират Дубай — ввиду высокого уровня цифровизации (обмен цифровыми данными, внедрение беспилотных транспортных средств, зона для деятельности поставщиков виртуальных услуг), а также КСА и КНР (из-за САР).

В-третьих, необходимо учитывать государственное устройство отдельных государств; хотя в большинстве случаев уголовное и уголовно-процессуальное право относится к исключительной компетенции федераций (например, ОАЭ), в Республике Индия указанное относится к конкурирующей сфере (список 3 к Конституции РИ от 26.11.1949 с поправками от 28.09.2023).

В-четвертых, в отдельных законах содержится оговорка о расширенном действии: «*В случаях, когда компьютерная или телекоммуникационная система используется в качестве средства совершения преступления и в данном законе не предусмотрено наказание за указанное деяние, оно должно быть применено в соответствии с соответствующими уголовными законами*» (Закон ИРИ 2009 г., ст. 19 Прокламации № 958/2016 ФДРЭ). Использование ИС, информационных систем, электронного сайта, оборудования ИТ для совершения преступлений может рассматриваться в качестве отягчающего обстоятельства (ст. 60 ФДЗ ОАЭ № 34-2021).

---

https://laws.boe.gov.sa/BoeLaws/Laws/LawDetails/57694209-3eed-46c7-a5d8-a9ed012761d4/1 (дата обращения: 25.03.2025).

[247] Yilma K.M., Abraha H.H. The Internet and Regulatory Responses in Ethiopia: Telecoms, Cybercrimes, Privacy, E-commerce, and the New Media // Mizan Law Review. 2015. № 9 (1). P. 108–153.

В-пятых, и в уголовно-процессуальном регулировании встречаются непосредственно (материальные) уголовно-правовые нормы или же отсылки к нему. Примером первого служат ст. ст. 660–661, 669, 670 Уголовно-процессуального закона ИРИ от 03.07.2013[248], касающиеся нескольких видов деяний: нарушений конфиденциальности или неприкосновенности частной жизни должностными лицами; совершения компьютерных преступлений в отношении систем электронного документооборота в уголовном судопроизводстве из-за неосторожной формы вины лиц, ответственных за поддержание безопасности центров, компьютерных и телекоммуникационных систем и информации; неисполнение судебных решений и охранных приказов о сохранении, раскрытии и предоставлении (электронных) данных с уведомлением обладателя информации.

Примером второго случая — примечание к ст. 652 указанного акта ИРИ: «*Судебные органы могут проводить судебные расследования и получать необходимую информацию через Национальную сеть правосудия. В этом случае государственные органы, негосударственные публичные учреждения и юридические лица обязаны объявить о необходимости реагировании через указанную выше сеть. Лицо, отклоняющееся от положений настоящего примечания, подлежит наказанию в соответствии со ст. 576 Исламского уголовного закона*[249]*…*».

Тем не менее ни одно законодательство нельзя назвать совершенным с учётом типологии киберугроз. В случае выявления, например, т.н. цифровых наркотиков предлагается привлекать лицо к ответственности за электронное мошенничество по киберзаконодательству и блокировать соответствующие веб-сайты на основании решений прокуратуры или суда в зависимости от предусмотренного порядка, поскольку действия не попадают под традиционное изготовление веществ или

---

[248] قانون آیین دادرسی کیفری مصوب ۱۲.۰۴.۱۳۹۲[Уголовно-процессуальный закон Ирана, принятый 12.04.1392] // База законодательства ИРИ. URL: https://www.davoudabadi.ir/9673250/قانون-آیین-دادرسی-کیفری (дата обращения: 04.04.2025).

[249] قانون مجازات اسلامی [Исламский уголовный закон] // Законодательная база. URL: https://davoudabadi.ir/page/5709812/قانون-مجازات-اسلامی (дата обращения: 19.04.2025).

создание веб-сайтов с целью торговли или пропаганды[250]. Это связано с тем, что на сегодняшний день ни один антинаркотический закон в мире не предусматривает криминализацию и пенализацию цифровых наркотиков, ведь наркотик определяется как объект материального мира и предусмотрен списками международных договоров.

С точки зрения **состава преступления** оговоримся, что в рассматриваемых государствах подходы к определению элементов разнятся. В арабских странах и Иране выделяется от двух до четырех составляющих (араб. «أركان», перс. «عناصر»): материальный (араб. «مادي», перс. «مادی»), моральный или психологический (араб. «معنوي», перс. «معنوی» или «روانی»), законодательный (араб. «قانوني», перс. «قانونی»). Причинно-следственная связь / причинность (араб. «سببية») также может выступать в качестве самостоятельного элемента, как указано в главе 2 Декрета-закона Королевства Бахрейн № 15 от 1976 года «О наказаниях» (далее — ДЗ Бахрейна № 15-1976)[251] или в комментарии к ст. 88–108 Модельного закона о преступлениях Лиги арабских государств[252], либо же составляющей материального[253]. Под материальным понимают само деяние, а моральный или психологический элемент выражается в предумышленности или умысле (араб. «عمد»)[254] и ошибке (араб. «خطأ»)[255], объединяющей знание (араб. «العلم») и волю (араб. «الإرادة»). Причинно-

---

[250] آل خطاب، خميس عبد ربه منشور. التكييف القانوني للمخدرات الرقمية على قيام المسؤولية الجزائية في التشريع الأردني // مجلة جامعة الحسين بن طلال للبحوث. ٢٠٢١. ٧ (٢). ١٧٠-٢٠٣ ص [Правовая характеристика цифровых наркотиков с точки зрения установления уголовной ответственности в законодательстве Иордании // Научно-исследовательский журнал Университета Аль-Хусейн бин Талал. 2021. № 7 (2). С. 170-203].

[251] مرسوم بقانون ١٥ لسنة ١٩٧٦ بإصدار قانون العقوبات [Декрет-закон Королевства Бахрейн № 15 1976 года «О наказаниях»] // Электронная база законодательства Королевства Бахрейн. URL: https://www.legalaffairs.gov.bh/Publications/Download/017.pdf (дата обращения: 31.01.2025).

[252] المذكرة التوضيحية للقانون الجزائي العربي الموحد الجزء الأول [Пояснительная записка к Модельному закону о преступлениях Лиги арабских государств: часть первая] // Электронная база единообразных арабских законов в рамках Лиги арабских государств. URL: http://www.lasportal.org/ar/legalnetwork/PublishingImages/Lists/TypicalArabLaws/AllItems/08.%20القانون%20الجزائي%20العربي%20الموحد.pdf (дата обращения: 05.02.2023).

[253] Вторая позиция отражена в юридической литературе. См. подробнее Siham L., Safia S. Legal criminal mechanisms for combating cybercrime in Algerian legislation // Russian Law Journal. 2025. № 1. P. 52–61.

[254] Может быть как общий, так и специальный. См. Там же.

[255] Под ошибкой понимается небрежность, отсутствие внимания, предосторожности, легкомысленность, безрассудство, неуважение или несоблюдение законов. См. подробней ст. 39 ФДЗ ОАЭ № 31-2021, ст. 24 ДЗ Бахрейна № 15-1976, ст. 32 Законе Катара № 11-2004.

следственная связь включает в себя материальную связь, которая начинается с действия, совершенного преступником, и связана умственно с тем, чего он должен ожидать с точки зрения обычных результатов своего действия [если оно совершено преднамеренно][256]. Похожим образом трактуется состав преступления и в Эфиопии: легальный элемент, *actus reus* (действия и бездействие), *mens rea* (вина)[257].

В Республики Индия, помимо классической англо-американской двухзвенной структуры, в юридической литературе отдельно выделяют лицо (англ. «person») и ущерб / вред (англ. «injury»)[258]. При этом, согласно п. 1 ст. 2 Бхаратия Ньяя Санхита (Закон Республики Индия № 45 от 25.12.2023), под деянием (англ. «act») понимается как одно, так и ряд действий[259]. Ранее, согласно ст. 32 Индийского уголовного кодекса (Закон Республики Индия № 45 от 06.10.1860)[260], термин «act» распространялся и на преступное бездействие (англ. «illegal omissions»). С точки зрения субъекта отметим, что *person* включает в себя как физическое, так и юридическое лицо — любая компания, ассоциация, объединение лиц вне зависимости от их регистрации (п. 26 ст. 2 Закона Республики Индия № 45 от 25.12.2023 совпадает с определением Закона Республики Индия № 45 от 06.10.1860). При этом специализированное регулирование может расширять данную категорию: физическое лицо, неразделённая индусская семья, фирма, компания; ассоциация, орган, объединение лиц вне зависимости от их регистрации; любое искусственное юридическое лицо, любое агентство, офис или филиал, принадлежащий или

---

[256] См. постановление Федерального Верховного суда ОАЭ № 367 от 2019 г., решение Кассационного суда APE по апелляции № 144 от 1995 г.); عبد الله ا.، سيد م. الأحكامُ الموضوعيَّة لجريمتي الإخفاء والعبث بالدليل الرقميّ في التشريعين الإماراتيّ والمصريّ (دراسة مُقارنة) // مجلة جامعة الشارقة للعلوم القانونية. ٢٠٢٤. ٢١. (٤. ١٧٦-١٩٨ ص. [Абдулла И., Сайид М. Основные положения о преступлениях сокрытия и фальсификации цифровых доказательств в законодательстве ОАЭ и Египта (сравнительное исследование // Журнал университета Шарджи юридических наук. 2024. № 21 (4). С. 176–198].

[257] Nirmala G.K., Ato Serkaddis Zegeye. Criminal law I. Teaching material. Justice and Legal System Research Institute, 2009. 286 p. URL: https://www.lawethiopia.com/images/teaching_materials/Criminal%20law%20I.pdf (accessed 25.03.2025). P. 167–210.

[258] Ghuman A. Elements of Crime // International Journal of Law Management & Humanities. 2018. № 1 (4). P. 1–18.

[259] Bharatiya Nyaya Sanhita 2023 // Ministry of Home Affairs: official website. URL: https://www.mha.gov.in/sites/default/files/250883_english_01042024.pdf (accessed 25.03.2025).

[260] The Indian Penal Code // Digital Repository of Laws. URL: https://www.indiacode.nic.in/repealedfileopen?rfilename=A1860-45.pdf (accessed 25.03.2025).

контролируемый любым упомянутым субъектом (п. «s» ст. 1 Закона Республики Индия № 15 от 17.01.2003 «Об отмывании денег»[261]). *Injury* подразумевает любой вред, незаконно причинённый лицу, его телу, разуму, репутации или имуществу (п. 4 ст. 2 Закона Республики Индия № 45 от 25.12.2023 совпадает с определением Закона Республики Индия № 45 от 06.10.1860).

Подход китайского правоприменителя и законодателя сроднен отечественному (объект, объективная сторона, субъект, субъективная сторона), хотя отмечается тенденция к одобрению германо-японского учения о трехэлементном составе преступления [262] . Исходя из уведомления ВНП КНР 2021 г., при расследовании сетевых преступлений устанавливается объективное поведение (кит. «客 观 行 为»), субъективные аспекты (кит. «主 观 方 面»), обстоятельства и последствия преступных действий (кит. «行为的情节和后果»).

Считается, что операционные записи, записи просмотра сети, логистическая информация, записи об урегулировании транзакций, информация о мгновенной связи отражают поведение с использованием технических средств и инструментов (с указанием информации об устройстве, ПО, системного журнала, доменном имени, Wi-Fi, географическом местоположении, IP-адрес, MAC-адрес терминала, базовой станции связи). К объективному поведению также относят взаимосвязь между способами осуществления, преступными деяниями и результатами.

Субъективные аспекты включают в себя изучение следующего: имеются ли субъективные и преднамеренные записи чата, опубликованный контент, записи просмотра лиц, подозреваемых в совершении преступлений; нарушает ли поведение подозреваемого в уголовном преступлении требования системных подсказок и нормальный процесс работы; используются ли программы, произведенные, используемые или предоставленные другим лицам подозреваемым в уголовном преступлении, в основном используются для незаконной и преступной

---

[261] The Prevention of Money-Laundering Act, 2002 // India Code: Digital Repository of Laws. URL: https://www.indiacode.nic.in/bitstream/123456789/2036/5/A2003-15.pdf (accessed 21.04.2025).
[262] Лун Ч. Состав преступления в уголовно-правовой доктрине Китая // Lex Russica. 2016. № 9. С. 129-135.

деятельности; нарушает ли объект, частота, сумма транзакций нормальную деловую практику; часто ли подозреваемый в преступлении использует скрытый доступ в Интернет, зашифрованную связь, уничтожение данных и другие меры или ложную личность.

К идентификационной сетевой идентичности (личности) относится информация об учетной записи и аутентификации личности, цифровая подпись, биометрическая информация и иные данные из социальных сетей, оплата и расчеты в онлайн-играх, в ходе электронной торговли, логистики и на других платформах. Записи о звонках, текстовых сообщениях, сообщениях в чате, документах, изображениях, аудио и видео также могут отражать личность преступника.

Записи в чате, записи о транзакциях и базе данных, аудио- и видеофайлы, информация о базе данных могут отражать незаконный доход, характер и количество полученных и распространяемых данных и документов. Количество аккаунтов, кликов, просмотров, переадресации и другой контент может отражать влияние преступных действий на порядок киберпространства. Количество затронутых компьютерных информационных систем, информация о журнале сервера могут отражать степень влияния преступных действий на работу информационной сети. Количество потерпевших, сумма материального ущерба, экономические потери, уничтожения информационных систем, степень ущерба для сетевого порядка, степень воздействия на репутацию могут отражать нарушение интересов личности или имущества потерпевших, а равно государства (ст. ст. 17–20 уведомления ВНП КНР 2021 г.).

В преамбуле Закона РИ № 1-2023 в качестве элементов преступления (индонез. «unsur») упомянуто деяние (индонез. «perbuatan») и психическое отношение (индонез. «sikap batin»). Как указывается в пояснительной записке к нему, выделяются объективные и субъективные факторы деяний. В доктрине разъясняется, что под первым понимаются действия или бездействие, последствия, обстановка и причинная связь, а под вторым — умысел или небрежность, цели.

Отметим, что определение преступления носит формальный характер, а потому запрет законом можно выделить в качестве отдельного элемента[263].

Конституирующими признаками киберпреступлений выступают средства или предметы посягательства: компьютеры, компьютерные / информационные / информационно-коммуникационные сети и системы, ИТ-средства; информационные / электронные / компьютерные данные и информация, ИТС «Интернет», электронные сайты, электронные почты, учётные записи, электронные документы и инструменты, электронные средства платежа, электронные подписи, цифровые сертификаты и валюты, а также виртуальные валюты и незаконный контент, носящий оскорбительный, порочащий или аморальный характер. Нанесение ущерба перечисленному является либо целью, либо последствием совершения преступления. В качестве последнего в норме также могут указаны возбуждение вражды или ненависти (экстремистская направленность), а равно вред интересам личности, государства, собственности, монотеистическим религиям и закону.

Отдельного внимания заслуживает правовая неопределённость в отношении неправомерного использования ИИ как орудия преступления: на основании решения Исполнительного совета Эмирата Дубай № 3 от 17.04.2019[264] внедрены беспилотные транспортные средства — «*законодательство, действующее в Эмирате, ... распространяется на действия, совершенные автономным транспортным средством и являющиеся преступлениями, за которые предусмотрено наказание для виновных*» (ст. 15 Закона Эмирата Дубай № 9 от 06.04.2023 «Об эксплуатации беспилотных транспортных средств в Эмирате

---

[263] Manthovani R. Implementation of Criminal Law in Indonesia // YURISDIKSI: Jurnal Wacana Hukum Dan Sains. 2021. № 16 (4). P. 266–274.

[264] قرار المجلس التنفيذي رقم ٣ لسنة ٢٠١٩ بشأن تنظيم التجربة التشغيليّة للمركبة ذاتيّة القيادة في إمارة دبي [Решение Исполнительного совета Эмирата Дубай № 3 от 17.04.2019 «Об организации эксплуатации беспилотных транспортных средств в Эмирате Дубай»] // Законодательный портал Дубай. URL: https://dlp.dubai.gov.ae/Legislation%20Ar%20Reference/2019/(3)%20رقم%20التنفيذي%20المجلس%20قرار%20بشأن%20تنظيم%20ذاتية%20القيادة%20مركبة%20تعمل%20بمُوجب%20نظام%20لسنة%202019%20.html#:~:text=ا%20نظام%20إلكتروني%20ذكي%20مُصمّم%20من,قيادتها&text=.لمُحاكاة,فيها%20المُواصفات%20التي%20تعتمدها%20الهيئة%20بدون%20أي%20تدخُّل%20بشري (дата обращения: 25.03.2025).

Дубай»[265]). Отметим, что хотя в КНР весьма активным образом с 2021 г. реализуется схожий проект с беспилотными транспортными средствами (БТС) в 17 зонах в 26 провинциях [266], в отношении вопросов ответственности нет единой законодательной позиции.

При этом «*любое преступление, предусмотренное уголовным или иным законом, которое совершается с помощью систем искусственного интеллекта, подлежит наказанию, предусмотренному для данного преступления*» (ст. 31 Закона Королевства Бахрейна от 29.04.2024 «О технологии искусственного интеллекта и её использовании»[267]).

Административное регулирование КНР от 13.07.2023 «Временные меры по управлению генеративными службами искусственного интеллекта» [268], разработанное Управлением киберпространства Китая, Национальной комиссией по развитию и реформам, Министерством образования, Министерством науки и технологий, Министерством промышленности и информационных технологий, Министерством общественной безопасности и Национальным управлением радио

---

[265] قانون رقم ٩ لسنة ٢٠٢٣ بشأن تنظيم تشغيل المركبات ذاتيّة القيادة في إمارة دبي [Закон Эмирата Дубай № 9 от 2023 г. «Об эксплуатации беспилотных транспортных средств в Эмирате Дубай»] // Законодательный портал Дубай. URL: https://dlp.dubai.gov.ae/Legislation%20Ar%20Reference/2023/%202023%لسنة%20(9)%20رقم%20قانون%20بشأن%20تنظيم%20تشغيل%20المركبات%20ذاتية%20القيادة.pdf (дата обращения: 25.03.2025).

[266] Баканов К.С., Васюков В.Ф. К вопросу о правовом регулировании эксплуатации беспилотных транспортных средств в отдельных странах Азии // Проблемы правоохранительной деятельности. 2024. № 3. С. 58–63.

[267] تقرير لجنة الشؤون التشريعية والقانونية بخصوص الاقتراح بقانون بتنظيم تقنيات الذكاء الاصطناعي واستخداماته، والمقدم من أصحاب السعادة الأعضاء: علي حسين الشهابي، وجمال محمد فخرو، والدكتورة جهاد عبدالله الفاضل، والدكتور محمد علي حسن علي، ودلال جاسم الزايد [Доклад Комитета по законодательным и правовым вопросам относительно предлагаемого закона о регулировании технологий искусственного интеллекта и их использования, представленный членами: Али Хусейном Аль-Шехаби, Джамалом Мухаммадом Фахро, доктором Джихадом Абдуллой Аль-Фадилом, доктором Мохаммедом Али Хасаном Али и Далалом Джассимом Аль-Зайедом] // Комитет по законодательным и правовым вопросам Маджлис Аш-Шура Королевства Бахрейн. URL: https://councilsessions-s3-bucket.s3.me-south-1.amazonaws.com/s28_06a_pdf-1714037459122.pdf?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIA4XAHVY3LHQ7YI5EO%2F20240929%2Fme-south-1%2Fs3%2Faws4_request&X-Amz-Date=20240929T150137Z&X-Amz-Expires=900&X-Amz-Signature=6638b015b246846cd3a70da306bc21b72a43f3a95a0022a61a553bb0172eec3b&X-Amz-SignedHeaders=host (дата обращения: 25.03.2025).

[268] 生成式人工智能服务管理暂行办法 [Временные меры по управлению услугами искусственного интеллекта поколений] // Управление КНР по киберпространству. URL: https://www.cac.gov.cn/2023-07/13/c_1690898327029107.html (дата обращения: 29.09.2024).

и телевидения и вступившее в силу 15.09.2023, является частью комплексного законодательства наряду с административными регулированиями КНР от 25.11.2022 «О глубоком синтезе в информационных услугах на основе Интернета» [269], вступившими в силу 10.01.2023, и «Об алгоритмах рекомендаций в информационных услугах на основе Интернета» [270], вступившими в силу 01.03.2022, и предусматривает ответственность поставщиков услуг по генеративному ИИ за нарушение законов о кибербезопасности, безопасности данных, прогрессе науки и технологий, защите персональных данных.

В арабском, персидском, английском и индонезийском языках юридические конструкции «каждый» / «любой» / «тот, кто»: араб. / перс. «كل» / «مرتكب جرمی شود»[271], англ. «whosoever», «any person», «person», индонез. «setiap organ»[272] — охватывают и физических (ФЛ), и юридических лиц (ЮЛ)[273]. Отдельными актами, в частности Законом Республики Индия № 21 от 09.06.2000 «Об информационных технологиях» (далее — Закон РИ № 21-2000)[274], предусматривается возможность привлечения к ответственности одновременно и ФЛ, и ЮЛ: «*…если нарушение… было совершено компанией, и доказано, что оно произошло с согласия или вследствие сговора или связано с любой халатностью со стороны любого директора (партнёра), менеджера, секретаря или другого сотрудника компании, лицо также считается виновным в нарушении и подлежит соответствию и*

---

[269] 生成式人工智能服务管理办法 [О глубоком синтезе в информационных услугах на основе Интернета] // Управление КНР по киберпространству. URL: https://www.cac.gov.cn/2023-04/11/c_1682854275475410.htm (дата обращения: 29.09.2024).

[270] 互联网信息服务算法推荐管理规定 [Об алгоритмах рекомендаций в информационных услугах на основе Интернета] // Государственный совет Китайской Народной Республики. URL: https://www.gov.cn/zhengce/zhengceku/2022-01/04/content_5666429.htm (дата обращения: 29.09.2024).

[271] Формулировка «совершает преступление» на персидском сопоставима с обозначенной конструкцией.

[272] Иногда под этим термином может пониматься физическое лицо и корпорация, которая в свою очередь необязательно является юридическим лицом, но и группа активов (ст. 1 Закона Республики Индонезия № 15 от 17.04.2002 «Об отмывании денег» в ред. 2010 г.).

[273] Волеводз А.Г., Цыплакова А.Д. Уголовная ответственность юридических лиц в Объединённых Арабских Эмиратах и Королевстве Саудовская Аравия: сравнение материальных и процессуальных аспектов// Российский следователь. 2024. № 3. С. 51–56.

[274] The Information Technology Act, 2000 // Digital Repository of Laws. URL: https://www.indiacode.nic.in/bitstream/123456789/1999/1/A2000-21%20%281%29.pdf#search=information%20act%202000 (accessed 19.03.2025).

наказанию». В качестве признаков для привлечения к ответственности также могут выступать действия «*за счёт или с использованием средств*» ЮЛ, а равно совершение «*в результате действий, грубой небрежности, согласия или сокрытия президента, члена совета директоров, директора или любого другого должностного лица*» (указ Султана Омана № 58 от 10.11.2024 «Закон о СМИ»[275]).

В качестве специального субъекта могут выступать администратор[276] или владелец электронного сайта или электронной учётной записи, владелец ключа шифрования, поставщик услуг (Интернет-услуг, в сфере кибербезопасности, услуг в сфере сети общественного пользования, цифровых услуг), цифровые издательские платформы, сервисный провайдер, посредник информационной сети, лицензиары, должностные лица, в частности имеющие электронные полномочия, предоставленные для доступа к постановлениям Министерства человеческих ресурсов и эмиратизации ОАЭ или иным документам, имеющие доступ к Национальной сети правосудия ИРИ.

В юридической научной литературе[277] ведутся дискуссии: как возможный субъект уголовной ответственности или предмет посягательства рассматриваются искусственный интеллект (ИИ) и аватары в метавселенной[278]. ИИ внедряется как

---

[275] مرسوم سلطاني رقم ٥٨ / ٢٠٢٤ بإصدار قانون الإعلام [Указ Султана № 58/2024 об обнародовании Закона о СМИ] // Законодательная база «Кануун». URL: https://qanoon.om/p/2024/rd2024058/ (дата обращения: 04.05.2025).

[276] Лицо, ответственное за организацию, управление, отслеживание или поддержку одного или нескольких сайтов в информационной сети, включая права доступа пользователей, дизайн, создание или организацию страниц или контента.

[277] См., например, Шестак В.А., Волеводз А.Г. Современные потребности правового обеспечения искусственного интеллекта: взгляд из России // Всероссийский криминологический журнал. 2019. № 13 (2). С. 197-206; Бессонов А. А. Искусственный интеллект в преступлении: орудие или субъект? // Расследование преступлений: проблемы и пути их решения. 2022. № 3(37). С. 28-32, Sayyed H. Artificial intelligence and criminal liability in India: exploring legal implications and challenges // Cogent Social Sciences. 2024. 10(1). 2343195; Purnomo H. Criminal liability for the use of artificial intelligence in Indonesia // Jurnal Info Sains: Informatika dan Sains. 2023. № 13 (3). P. 1109–1114; CS Chaitali J. C.S., Rathor S.P. A Legal Framework for Determining The Criminal Liability And Punishment For Artificial Intelligence // Tuijin Jishu/Journal of Propulsion Technology. 2024. № 45 (1). P. 807–820.

[278] القاضي ر. الدليل الجنائي الرقمي في تقنية الميتافيرس // المجلة العربية للدراسات الأمنية. ٢٠٢٣. ٣٩ (٢). ١٨٩-٢٠٤ ص. [Аль-Кади Р. Цифровые судебные доказательства в технологии Metaverse // Арабский журнал исследований в области безопасности. 2023. № 39(2). С. 189–204].

البلوي غ. الأبعاد القانونيَّة لاستخدام الروبوتات في الأعمال الإرهابية في النظام السعودي // المجلة العربية للدراسات الأمنية.٢٠٢٤. ٤٠ (١). ٤-١٣ ص [Аль-Балави Г. Правовые аспекты использования роботов в террористических

на уровне отдельных секторов (e.g., система государственных услуг в Катаре), так и в рамках урбанизации. В то время как «Умный Дубай» (араб. «دبي الذكية», англ. «Smart Dubai») и «Город Султана Хэйтам» (араб. «مدينة السلطان هيثم», англ. «Sultan Haitham City») являются лишь способом управления отдельными элементами инфраструктуры существующего города через Интернет вещей — цифровыми двойниками, «Ниум» / «Неом» (араб. «نيوم», англ. «NEOM») предполагает полностью цифровую среду, управляемой ИИ в рамках метавселенной [279] . Возникают вопросы, связанные с возможными ошибками, методами устранения последствий и субъектом ответственности в рамках исламского шариата.

На основании Положений «О Саудовском управлении промышленных городов и технологических зон» (решение Совета министров № 235 от 26.03.2001) [280] и «Об Управлении экономических городов (Управлении специальных экономических городов и зон)» (указ короля КСА № A/19 от 23.02.2010) [281] промышленные города (араб. «المدن الصناعية»), технологические зоны (араб. « مناطق التقنية») (ПГ/ТЗ), специальные экономические города и зоны (араб. « المدن والمناطق الاقتصادية الخاصة») (СЭГ/З) имеют особые статусы в части корпоративного, трудового и налогового права, и действующие в их пределах субъекты попадают под правовое

актах в системе Саудовской Аравии // Арабский журнал исследований безопасности. 2024. № 40(1). С. 4–13].

[279] В начале 2023 г. платформа «Sandbox» и Управление цифрового правительства КСА подписали меморандум о взаимопонимании для разработки подходящей технологии метавселенной для города. Мохаммад Сулейман, Салах Газаль, Винсент Карчеди, Адель Аль-Адави. Указ. Соч. С. 19.

[280] تنظيم الهيئة السعودية للمدن الصناعية ومناطق التقنية [Положение о Саудовском управлении промышленных городов и технологических зон] // Бюро экспертов Совета министров КСА. URL: https://laws.boe.gov.sa/BoeLaws/Laws/LawDetails/f9bd197e-980e-4e9f-948c-a9a700f2994e/1 (дата обращения: 25.03.2025).

[281] تنظيم هيئة المدن الاقتصادية (هيئة المدن والمناطق الاقتصادية الخاصة) [Положение об Управлении экономических городов (Управлении специальных экономических городов и зон)] // Бюро экспертов Совета министров КСА. URL: https://laws.boe.gov.sa/BoeLaws/Laws/LawDetails/4100e06a-1a43-458d-a3b4-a9a700f1e3d9/1 (дата обращения: 25.03.2025).

регулирование уполномоченных органов[282]. Для «Ниум», управляемого в будущем исключительно ИИ, будет выработано отдельное регулирование[283].

Существующая нормативно-правовая база не даёт точного ответа: информационные технологии оцениваются, исходя из принципа публичного интереса или *масляхатун* (араб. «مصلحة») [284] . Представляется возможным применение договора *вакяялятун* (араб. «وكالة»), то есть представительства субъекта, отвечающего за разработку и мониторинг системы — человека[285]. Однако и здесь однозначно невозможно определить ответственного, элементы *'акд* (с араб. «عقد» — соглашение): оферту и акцепт, — а также агентскую форму[286].

«Ниум» — мегапроект, существующий в значительной мере за счёт иностранных инвестиций, привлечение которых одобряется Министерством инвестиций (бывшим Генеральным инвестиционным управлением Саудовской Аравии), что предшествует инкорпорации (учреждению) компании. В рамках СЭГ/З и ПГ/ТЗ компании являются общества с ограниченной ответственностью (англ. «LLC»; араб. «الشركة ذات المسؤولية المحدودة»), либо учреждаются совместные предприятия (араб. «مشروع مشترك»). После выполнения положений и различных регистраций (в Министерстве человеческих ресурсов и социального развития, Управлении по вопросам закята, налогов и таможни, Общей организации

---

[282] Например, в марте 2021 года Главное управление гражданской авиации Саудовской Аравии опубликовало специальные налоговые ставки и правила для Интегрированной зоны логистики — первой специальной экономической зоны Королевства. См. подробнее SAUDI ARABIA: Rules Released for Kingdom's First Special Economic Zone // HKTDC. 07.04.2021. URL: https://research.hktdc.com/en/article/NzE0ODY3Nzc2 (accessed 25.03.2025); Saudi Arabia Regulatory Update: Four new special economic zones launched // Clyde&Co. 27.04.2023. URL: https://www.clydeco.com/en/insights/2023/04/saudi-arabia-regulatory-update-economic-zones (accessed 25.03.2025).

[283] NEOM 'fully under Saudi sovereignty, regulations,' says government official refuting inaccurate media reports // Arab news. 16.05.2022. URL: https://www.arabnews.com/node/2082796/business-economy (дата обращения: 25.03.2025).

[284] О концепции *масляхатун* см. подробнее Kamali M. H. Principles of Islamic jurisprudence (Ushul al-Fiqh). Cambridge: Islamic Texts Society, 1991.

[285] О концепции *вакяялятун* см. подробнее Al-Shibli K. Agency (Wakala) and its applications in Islamic banking // Journal of Islamic Economics, Banking and Finance. 2020. № 16(3). P. 1-15.

[286] Об общих началах *'акд* см. подробнее Kamali M.N. The principles of Islamic jurisprudence. Cambridge Scholars Publishing, 2018. 550 p.

О формах агентского договора см. подробнее Vladeck D.C. Machines without principals: Liability rules and artificial intelligence // Washington Law Review. 2014. № 89(1). P. 117-150.

социального страхования, почте и торговых палатах) выдается нотариально заверенное свидетельство о коммерческой регистрации Министерством коммерции и промышленности. По общему правилу компании находятся под надзором Управления по рынку капитала Саудовской Аравии. Однако деятельность юридических лиц, действующих в рамках «Ниум», является предметом надзора Управления специальных экономических городов и зон.

Сам проект «Ниум» осуществляется под руководством закрытой акционерной компании под названием «NEOM CO» / «شركة نيوم» (араб. « شركة مساهمة مقفلة»), которая создана в 2019 г. и принадлежит Государственному инвестиционному фонду Саудовской Аравии.

Атрибутировать отдельные элементы правосубъектности ИИ, равно как и уравнивать в их статусе подобно юридических лицам с учётом принципов исламского шариата и особенностей правовых систем арабских стран без разработки специального регулирования довольно опрометчиво [287]. Требуется *мухтасиб*[288], который бы следил за «праведностью» (правильностью) алгоритма, этичностью их программирования с целью соблюдения принципов справедливости, прозрачности и благосостояния уммы, отвечая *макасыду аш-шариа'ти* (с араб. «مقاصد الشريعة» буквально — целям шариата)[289].

Способности системы ИИ оценивать и принимать решения нельзя доверять, поскольку она не обладает сознательной и различающей свободой воли, которая является решающим элементом, определяющим уголовную ответственность. ИИ можно запрограммировать на действия по заранее определённым правилам. Однако он не может постичь глубинный смысл этих понятий и выносить

---

[287] Vicente A., Lavazza A. Artificial intelligence, legal personhood and the non-reductive materialist perspective // International Journal of Law and Information Technology. 2020. № 28(2). P. 146-162.

[288] Араб. «محتسب» происходит от араб. «حسبة» — *хисба / хисбатун* — и покоится на принципе «предписывать добро и запрещать зло» (араб. «ٱلْأَمْرُ بِٱلْمَعْرُوفِ وَٱلنَّهْيُ عَنِ ٱلْمُنْكَرِ»).

[289] О концепции *хисбатун* см. подробнее 'Abd al-Rahmān b. Nasr al-Shayzarī. The Book of the Islamic Market Inspector. Oxford University Press, 2004. 224 p.

О концепции *макасыду аш-шариа'ти* см. подробнее Kamali M.N. Maqasid al-Shariah made simple. International Institute of Islamic Thought, 2008. 32 p.

интерпретирующие суждения[290]. Подобные суждения справедливы не только для стран религиозной правовой семьи, но и для иных государств, относящихся к Глобальному Югу, поскольку в виртуальном мире фактически имеет место единство субъекта и объекта[291].

По этой причине на данный момент ответственным за правонарушения, в частности уголовно наказуемые, будет юридическое лицо, осуществляющее администрирование проектом или непосредственную экономическую деятельность, в зависимости от последствий совершенного деяния [292]. В юридической литературе отмечается, что субъектом преступления могут выступать дизайнер, программист, разработчик, производитель, оператор, владелец и пользователь[293].

В качестве применимых к физическим лицам **наказаний** выступают как связанные, так и не связанные с лишением свободы: штраф, увольнение с государственной службы (ИРИ), конфискация [294] , депортация, блокировка электронной подписи (Катар).

Фактически электронные преступления относятся к категории *тазир*, а потому к ним не применяются специфические наказания, предусмотренные исламским шариатом. В Бахрейне лишение свободы не превышает года, а штрафы — до 30 тыс. динар (примерно 6,7 млн рублей); Государстве Катар — от 1 года до 3 лет; от 100 тыс. до 500 тыс. катарских риалов (примерно 2,32 млн – 11,6 млн

---

[290] El-Kady R. Artificial intelligence and criminal law. In: Artificial Intelligence Approaches to Sustainable Accounting / ed. M. Tavares, G. Azevedo, J. Vale, R. Marques, M. Bastos. IGI Global, 2024. P. 34–52; El-Kady R. Investigating forensic evidence in metaverse: a comparative analytical study. In Forecasting Cyber Crimes in the Age of the Metaverse / ed. H. Elshenraki. IGI Global, 2024. P. 227–258; El-Kady R. Navigating the legal maze: electric self-driving cars and the complexities of criminal law. Solving Fundamental Challenges of Electric Vehicles / ed. M. Shaik. IGI Global, 2024. P. 215–247.

[291] О единстве субъекта и объекта см. Титова Е.В. Общие методологические подходы к исследованиям в сфере цифрового права / Цифровое право: учебник / под ред. Э.Л. Сидоренко. М.: Юрлитинформ, 2024. С. 120.

[292] Подробнее об уголовной ответственности юридических лиц см. Волеводз А.Г., Цыплакова А.Д. Уголовная ответственность юридических лиц в Королевстве Саудовская Аравия // Российский следователь. 2023. № 11. С. 57-61.

[293] El-Kady R. Artificial Intelligence from the Criminal Law Perspective. Proceedings of the 10th International Conference on Advanced Intelligent Systems and Informatics 2024. Springer Nature, 2025. P. 162–173.

[294] В отдельных случаях выступает в качестве наказания (Тунис), в иных — как отдельная уголовно-процессуальная мера (КСА, ОАЭ, ИХК, ИРИ).

рублей)[295]; Государстве Кувейт — до 7 лет; до 50 тыс. кувейтских динаров (примерно 13,7 млн рублей); Султанате Оман — от полугода до 3 лет; до 150 тыс. оманских риалов (примерно 32 млн рублей); ОАЭ — до 5 лет; 3 млн эмиратских дирхамов (примерно 69 млн рублей); КСА — до 10 лет; до 5 млн саудовских риалов (примерно 112 млн рублей). Срок лишения свободы за нарушения Закона ИХК № 17 «Об электронных преступлениях» от 2023 г.[296] предусматривает и нижний, и верхний пределы — от 3–6 мес. до 3-х лет; штраф варьируется от нескольких до 45 тыс. иорданских динаров (примерно 5,4 млн рублей).

В Республике Индия нарушения Закона РИ № 21-2000 содержат наказания в виде лишения свободы сроком до 7 лет и штрафа размером до 1 млн рупий (примерно 920 тыс. рублей). Исключением является кибертерроризм, за который предусмотрено пожизненное лишение свободы, и нарушения приказов о сохранении информации посредниками — 2,5 млн рупий (примерно 2,3 млн рублей); приказов о мониторинге и сборе данных о траффике или информации — 10 млн рупий (примерно 9,2 млн рублей). В случае нарушения приказа о мониторинге, перехвате или расшифровке информации, а равно о запрете общего доступа к запрещённому контенту нет указания на конкретный размер штрафа.

В ИРИ многообразны общеуголовные наказания, включающие различные запреты, конфискацию, удары плетью, лишение социальных прав, публикацию приговоров в СМИ; размер штрафа за компьютерные преступления варьируется от 1 млн до 60 млн иранских риалов (примерно 2 тыс. – 120 тыс. рублей); срок лишения свободы за них — от 91 дня до 2-х лет. При этом преступления, совершенные специальным субъектом, в частности должностными лицами, наказывается штрафом размером до 1 млрд. иранских риалов (примерно 20 млн рублей), лишением свободы до 5 лет, увольнением со службы и запретом занимать определённые должности сроком до 5 лет.

---

[295] Наказание удваивается в случае совершения должностным лицом.

[296] قانون الجرائم الإلكترونية رقم ١٧ لسنة ٢٠٢٣ / الجريدة الرسمية. ٢٠٢٣. ١٢/٩. ٢٠٢٣. ص ٣٥٧٩ [Закон № 17 об электронных преступлениях от 2023 г. // Официальный вестник. 2023. 12.09.2023. С. 3579].

В отношении юридических лиц есть либо формальное (Кувейт), либо прямо предусмотренное сопоставление наказаний (ИРИ). Например, срочное лишение свободы эквивалентно временному закрытию: максимальное лишение свободы сроком до 5 лет равно временному приостановлению деятельности ЮЛ сроком 1–9 месяцев, а при рецидиве — сроком 1–5 лет; при максимальном лишении свободы сроком свыше 5 лет — 1–3 года временного закрытия ЮЛ, а при рецидиве — ликвидация (ст. 19 Закона ИРИ 2009 г.)[297]. Прокламация ФДРЭ № 958/2016 же предусматривает только применение штрафов в размере 50 000–500 000 эфиопских быр (примерно 32 тыс. – 320 тыс. рублей) по отношению к ЮЛ.

Без ущерба для уголовной ответственности аффилированного с ним физического лица юридическое лицо наказывается штрафом в размере до 1 000 000 млн катарских риалов (примерно 23,23 млн рублей), если одно из преступлений, предусмотренных Законом Катара № 14-2014, совершено от его имени или за его счёт. Судебной практикой ряда арабских государств и регулированием ИРИ также признано наложение уголовной ответственности на ЮЛ при совершении деяния в его пользу (ОАЭ, Кувейт)[298].

В законопроекте ТР № 036/2024 «О кибербезопасности» фактически субъектами выступают:

- специальные субъекты — ответственный за жизненно важный орган или критическую инфраструктуру, предоставляющий услуги по аудиту безопасности информационных систем или кибербезопасности — штрафы в размере от 30 до 60 тыс. тунисских динаров (примерно 815 тыс.–1,63 млн рублей);

- юридические лица: подрядчик по сети общественного транспорта, интернет-провайдер, поставщик услуг по кибербезопасности, поставщик цифровых услуг или создатель Интернет-платформы — штрафы в размере от 20 до 40 тыс. тунисских динаров (примерно 543 тыс.–1,1 млн рублей).

---

[297] Отметим, что именно за компьютерные преступления есть ряд специфических наказаний, не предусмотренных общеуголовным законом. См. Цыплакова А.Д., Васюков В.Ф. Уголовная ответственность юридических лиц в Исламской Республике Иран: особенности законодательства и правоприменения // Теория и практика общественного развития. 2025. № 6 (206). С. 211–219.

[298] Волеводз А.Г., Цыплакова А.Д. Уголовная ответственность юридических лиц в Объединенных Арабских Эмиратах // Российский следователь. 2023. № 12. С. 58-62.

При этом отметим **сочетание** начал административной и уголовной ответственности в отношении юридических лиц. Например, согласно пояснительной записке к законопроекту Королевства Бахрейн «О технологии искусственного интеллекта и её использовании», представленной на сессии 24.04.2024, предусмотренные наказания свидетельствуют о возможности вменения как административного правонарушения[299], так и уголовно наказуемого деяния (араб. «الأفعال المجرمة»). То же самое касается регулирования отдельных видов лицензирования (телекоммуникаций и СМИ[300]) и защиты персональных данных. (Письменное) предупреждение, отзыв лицензии, *административный* штраф[301], временное приостановление и/или прекращение доступа к электронной системе[302], временное приостановление деятельности, отказ от услуг (индонез. «pencabutan layanan») и принудительные полицейские меры (индонез. «daya paksa polisional»)[303] с возможной публикацией правонарушения на веб-сайте министерства по решению Министра юстиции и прав человека Республики Индонезия[304] налагаются

---

[299] На арабском «الجزاءات الإدارية» указано буквально «административная ответственность».

[300] См. например, ст. 38 Положения Королевства Саудовская Аравия от 29.11.2000 «О печати и публикациях» и Постановление Совета министров ОАЭ № 42 от 16.04.2025 «О регулировании административных правонарушений и наказаний, связанных с регулированием деятельности средств массовой информации». نظام المطبوعات والنشر [Положение «О печати и публикациях»] // Библиотека Министерства СМИ Королевства Саудовская Аравия. URL: https://www.media.gov.sa/sites/default/files/2020-06/نظام%20المطبوعات%20والنشر.pdf (дата обращения: 15.02.2025); قرار مجلس الوزراء رقم (42) لسنة 2025 بشأن لائحة المخالفات والجزاءات الإدارية المرتبطة بتنظيم الإعلام [Постановление Совета министров ОАЭ № 42 от 2025 года «О регулировании административных правонарушений и наказаний, связанных с регулированием деятельности средств массовой информации»] // Совет ОАЭ по СМИ. URL: https://uaemc.gov.ae/violations-and-penalties/ (дата обращения:21.06.2025).

[301] Характерно для всех изучаемых стран Глобального Юга.

[302] Применимо к организаторам электронных систем, согласно ст. 16Б Закона Республики Индонезия № 11 от 02.01.2024 «О внесении изменений в Закон № 11 2008 г. об электронной информации и транзакциях». См. Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik [О внесении изменений в Закон № 11 2008 г. об информации и электронных сделках] // Законодательная база Республики Индонезия. URL: https://peraturan.bpk.go.id/details/274494/uu-no-1-tahun-2024 (дата обращения: 04.05.2025).

[303] Правоприменение, осуществляемое сотрудниками, не являющимися полицейскими.

[304] Ст. ст. 225, 228 решения Министра коммуникаций и информатики Республики Индонезия № 5 от 01.04.2021 «О внедрении телекоммуникаций» (министерское решение № 5-2021 РИ). Peraturan Menteri Komunikasi dan Informatika Nomor 5 Tahun 2021 tentang Penyelenggaraan Telekomunikasi [Решение министра коммуникаций и информатики номер 5 от 2021 года о внедрении телекоммуникаций] // Министерство коммуникаций и информатики Республики Индонезия: официальный сайт. URL: https://jdih.komdigi.go.id/produk_hukum/view/id/768/t/peraturan+menteri+komunikasi+dan+informatika+nomor+5+tahun+2021 (дата обращения: 04.05.2025).

уполномоченными органами в соответствующей сфере (в арабских странах, например, Управлением по ИИ КБ, Комиссией КСА по информационно-коммуникационным технологиям, Министром транспорта, связи и информационных технологий СО), в то время как приостановка или запрет деятельности, *уголовно-правовые штрафы*, временное или полное закрытие предприятия, конфискация, в том числе оборудования, программного обеспечения, — только по решению суда при вынесении обвинительного приговора, в том числе с его публикацией в СМИ.

Как **отягчающие** наказание обстоятельства рассматриваются совершение во время или из-за выполнения работы, за счёт или в интересах иностранного государства, враждебной или террористической группы, а равно незаконной организации (ФДЗ ОАЭ № 34-2021), с целью нарушения общественного порядка, создания угрозы безопасности общества, нанесения вреда национальной безопасности страны или её экономическому положению, воспрепятствования или затруднения осуществления полномочий государственными органами, нарушения положений Конституции, нормативных правовых актов, нанесения вреда национальному единству и социальному миру (Закон АРЕ № 175-2018 «О борьбе с преступлениями в области информационных технологий»), способствование совершению другого преступления, ущерб секретам народного хозяйства (Закон Королевства Марокко № 07.03 от 22.12.2003 «Об автоматизированных системах обработки данных»), а равно посягательство на информацию, определённую уполномоченным органом как совершенно секретную, в военных интересах или в целях дипломатических (внешних) сношений; в случае, если страна находится в состоянии чрезвычайного положения или его угрозы (Прокламация ФДРЭ № 958/2016).

В зависимости от рассматриваемого государства и момента основанием в качестве **освобождения** от наказания (ответственности) может выступать активное сотрудничество, в частности ведущее к раскрытию преступления, изобличению его исполнителей, доказыванию их причастности или аресту хотя бы одного из них. К первому случаю относится АРЕ (после обнаружения деяния) и ОАЭ, второму —

АРЕ (до обнаружения деяния). При этом по Закону РИ № 21-2000 посредник не несёт ответственности за любую информацию, данные или коммуникационную связь третьих лиц, предоставленную или размещённую им за исключением двух случаев: посредник вступил в сговор или подстрекал, помогал или склонял угрозами, обещаниями либо иным образом к совершению противоправного деяния; получив фактические сведения или получив уведомление от соответствующего правительства или его ведомства о том, что любая информация, данные или канал связи, находящиеся в компьютерном ресурсе, контролируемом посредником, или подключенные к нему, используются для совершения противоправного деяния, посредник не удаляет или не отключает доступ к этому материалу на данном ресурсе в срочном порядке, не обжалуя доказательства каким-либо образом.

С точки зрения **юрисдикционных принципов** отметим традиционные: территориальный и экстратерриториальные (активный и пассивный персональные и реальный)[305]. При этом прослеживаются и неординарные подходы. Например, иранские суды имеют полномочия рассматривать дела в следующих случаях:

- сведения, используемые для совершения преступления, которые каким-либо образом хранятся в компьютерных и телекоммуникационных системах или на носителях данных, расположенных в пределах территориальной, морской и воздушной юрисдикции Исламской Республики Иран;

- преступление совершается через веб-сайты с доменом верхнего уровня с кодом страны Иран «.ir»;

- преступление, совершенное гражданином Ирана или иным лицом за пределами Ирана против компьютерных и телекоммуникационных систем и веб-сайтов, используемых или контролируемых тремя ветвями власти или руководством либо официальными государственными органами или любым учреждением или организацией, предоставляющими государственные услуги, или

[305] Шестак В.А., Цыплакова А.Д. Проблемы регулирования уголовной юрисдикции в Объединённых Арабских Эмиратах // Российский следователь. 2023. № 7. С. 65–68, Шестак В.А., Цыплакова А.Д. Проблемы регулирования уголовной юрисдикции в Королевстве Саудовская Аравия // Мировой судья. 2023. № 2. С. 2–6.

против веб-сайтов с доменом верхнего уровня с кодом страны Ирана «.ir» в крупном масштабе;

- компьютерные преступления, связанные с насилием над лицами, не достигшими восемнадцатилетнего возраста, независимо от того, является потерпевший или преступник гражданином Ирана или нет, а преступник находится на территории Ирана (ст. 664 Уголовно-процессуального закона ИРИ от 03.07.2013).

Ст. 15 Закона АНДР № 04-09 от 16.08.2009 «Специальные правила по предупреждению и борьбе с преступлениями, связанными с информационно-коммуникационными технологиями» (далее — Закон АНДР № 04-09) [306] расширяются пределы уголовной юрисдикции в отношении указанного вида деяний в случае, если преступник является иностранцем и посягательство направлено на алжирские государственные институты, национальную оборону или стратегические интересы национальной экономики.

Отметим, что регулирование законов о персональных данных и электронной информации зачастую носит экстратерриториальное действие и распространяется на лиц, государственные органы и международные организации, находящиеся за пределами юрисдикции государства, но правовые последствия попадают под неё и/или касается субъектов персональных данных (являющихся гражданами страны). Примером служит Закон Республики Индонезия № 27 от 17.10.2022 «О защите персональных данных» [307] . Доктрина эффекта применима и в случаях, если действие или поведение, составляющие преступление или нарушение, совершенные за пределами РИ, связаны с телекоммуникационными услугами, предоставляемыми в Индии, или телекоммуникационным оборудованием, или

[306] Закон № 04-09 от 25 шабан 1430 года хиджра, что соответствует 16 августа 2009 г. «Специальные правила по предупреждению и борьбе с преступлениями, связанными с информационно-коммуникационными технологиями» // Официальный вестник Алжирской Республики. 2009. № 47. С. 5–8 (на араб. яз.).

[307] Undang-undang (UU) Nomor 27 Tahun 2022 Pelindungan Data Pribadi [Закон № 27 «О защите персональных данных» 2022 г.] // Официальная база законодательства РИ. URL: https://peraturan.bpk.go.id/Details/229798/uu-no-27-tahun-2022 (дата обращения: 27.04.2025).

телекоммуникационной сетью, расположенной в Индии (ст. 50 Закона Республики Индия № 44 от 24.12.2023 «О телекоммуникациях»[308]).

При этом нигде, кроме Арабской конвенции, не предусмотрен порядок приоритетности принципов установления уголовной юрисдикции: защитный, собственно территориальный и активный персональный (ст. 30).

Таким образом, характеризуя уголовно-правовое содержание киберпреступлений в отдельных государствах Глобального Юга, отметим, что даже в рамках одного региона (будь то арабского, азиатского или африканского) нет единой позиции ни при определении, ни при наполнении рассматриваемых посягательств (см. Приложение № 1) и принимаются скорее формальные определения (если таковые вообще приняты на законодательном уровне). Опыт различных стран зависит от устоявшегося понятийного аппарата на период принятия нормативных правовых актов и имплементации международных договоров, источников права, характерных киберугроз, языковых и лингвистических особенностей, оказывающих влияние на юридическую технику в рамках одного семантического поля, историко-культурного и технического развития государств и их суверенных интересов, затрагивая иногда те предметы правоотношений, которые далеко не всегда имеют однозначный правовой статус (в частности, виртуальные активы, Блокчейн, мета-вселенные и искусственный интеллект).

В международно-правовых документах на региональном и универсальном уровнях можно выявить скорее виды и синонимичные понятия. Фактически на сегодняшний день киберпреступления — это использование ИТ, системы или сети в преступных целях, то есть запрещённые законом деяния, совершаемые в отношении или с использованием компьютерной (информационной) системы или виртуального пространства — т.н. современных высоких технологий. Они охватывают посягательства на данные, информационные сети и системы (в т.ч. АСОД), личность (её честь и достоинство), цифровые объекты (документы

[308] Telecommunications Act 2023 // India Code: Digital Repository of Laws. URL: https://www.indiacode.nic.in/bitstream/123456789/20101/1/A2023-44.pdf (accessed 10.05.2025).

идентификации, в том числе подписи, печати и сертификаты, электронные средства платежа и виртуальные активы, электронные документы), права интеллектуальной собственности, интересы потребителей, охраняемые законом тайны, правонарушения регулирования телекоммуникационного сектора, лицензионных видов деятельности, оказания сертифицированных услуг, правила пользования социальными сетями, мессенджерами, средствами связи и публикаций, в том числе электронной рекламы и контента, ЭДО в государственном и частном секторах, обеспечения безопасности объектов критической (информационной) инфраструктуры, удалённой работы, оказания государственных услуг, электронного голосования, электронной торговли и юридической деятельности. В широком смысле слова киберпреступления — это использование высоких технологий в преступных целях.

Отметим наличие нескольких подходов при классификации киберпреступлений в рассматриваемых странах Глобального Юга: законодательный, доктринальный и правоприменительный. Первый наиболее полно представлен в Приложении № 3; второй опирается на историю криминализации и пенализации деяний в конкретном государстве, расширяя исходя из состава преступления, восполняя возможные проблемы и обобщая опыт по регионам; третий тяготеет ближе к тому, что обозначается как типология преступлений. Последняя имеет тенденции к смешению фокуса от т. н. традиционных компьютерных преступлений (в том числе экономических, то есть на имущество) к посягательствам в виртуальном пространстве (конфиденциальность, государственную и общественную безопасность). С точки зрения типологии превалируют мошенничества, кибератаки и распространение деструктивного, порочащего или запрещённого контента (в том числе в террористических и экстремистских целях), понимание которого разнится от страны к стране. Перечисленные явления должны учитываться и ложиться в основу составов преступлений, запрещаемых национальными уголовными законами и/или охватываемых международными договорами. В то время как первые два и посягательства на данные охватываются всеми рассмотренными конвенциями и

соглашениями (см. Приложение № 4), отдельные специфические явления по типу цифровых наркотиков и электронных мух не учтены вовсе.

Рассмотренные юрислингвистические особенности позволяют расширить понятие киберпреступлений с точки зрения охватываемых составов и субъектов. Ввиду разности определения составов преступлений количество элементов, подлежащих доказыванию, варьируются от двух до пяти. С учётом разграничения административной и уголовной ответственности, отличного от отечественного подхода, в том числе за правонарушения в сфере лицензирования, не только суд может выступать в качестве компетентного органа, налагающего наказания за киберпосягательства. Наказания могут назначаться как традиционные (штраф, лишение свободы), так и специфические, характерные для конкретного государства и/или вида деяний (увольнение с государственной службы, конфискация, депортация, блокировка электронной подписи, временное приостановление или срочный запрет на осуществление деятельности ЮЛ, его ликвидация). В изучаемых странах предусмотрены как традиционные, так и специфические юрисдикционные принципы для распространения на виртуальное пространство.

Трансграничность киберпреступлений в смысле любого использования ИКТ в преступных (противоправных) целях ставит под вопрос существующие юрисдикционные привязки и типологически столь широко, что требует достаточно (а порой и, возможно, излишне) высокого уровня абстракции при выработке подхода (в общем) и отдельных мер (в частности) для того, чтобы законодатели и правоприменители, а не преступники были на шаг впереди. Хронологически (2000-е – 2010-е гг.) именно криминализация и пенализация, а также выработка доктринального и правоприменительного подходов служат основой для противодействия киберпреступлениям.

ГЛАВА II. КРИМИНОЛОГИЧЕСКАЯ ХАРАКТЕРИСТИКА ПРОТИВОДЕЙСТВИЯ КИБЕРПРЕСТУПЛЕНИЯМ В ОТДЕЛЬНЫХ СТРАНАХ ГЛОБАЛЬНОГО ЮГА

§ 1. Руководящие документы в сфере противодействия киберпреступлениям в отдельных странах Глобального Юга

Отметим, что озабоченность в сфере кибербезопасности на региональном и национальном уровнях стала активно обсуждаться в значительной мере с 2010-х гг. Об этом свидетельствуют, во-первых, активная разработка и принятие как законов, криминализующих и пенализирующих соответствующую категорию деяний, так и политик на уровне созданных компетентных государственных органов именно с этого периода. Во-вторых, с появлением уполномоченных структур в государствах Глобального Юга возникла идея о проведении министерских и других встреч для обсуждения единообразного подхода к киберпреступности и разработке инструментов для оценки и повышения уровня кибербезопасности с учётом возможного наличия иностранного элемента при совершении посягательств и стирания границ в виртуальном пространстве.

Арабский Восток. В юридической литературе высказывается мнение о том, что в ССАГПЗ есть стратегия борьбы с киберпреступностью[309]. Тем не менее на самом деле проводилось комплексное научное исследование «Электронные преступления в обществе Залива и как им противостоять» победителем премии принца Наифа бин Абдель Азиза за исследование в области безопасности за 2015 год — Академией полицейских наук султана Кабус (Султанат Оман, Низва)[310]. В нём описана типология растущих угроз и общие меры по защите государственных интересов в сфере кибербезопасности. Схожая ситуация и в ЛАГ, однако, в отличие от арабских объединений, в азиатском регионе разработано значительно больше документов.

---

[309] Salem F., Fiscbach T. Указ. Соч. С. 6.

[310] الجريمة الإلكترونية في المجتمع الخليجي وكيفية مواجهتها [Электронные преступления в обществе Залива и как им противостоять]. Эр-Рияд: Генеральный секретариат Совета сотрудничества арабских государств Персидского залива, 2016. 208 с. URL: https://www.gcc-sg.org/ar-sa/CognitiveSources/DigitalLibrary/Lists/DigitalLibrary/%الالكترونية%20الجريمة%20الأمنية/كتاب%20البحوث%20سلطنة%20عمان20.pdf (дата обращения: 25.03.2025).

После проведения Арабского высокого форума по кибербезопасности (Тунис, 21–22.10.2021) и запуска проекта «Арабское видение кибербезопасности» [311] была разработана арабская стратегия по кибербезопасности 2023–2027 гг.[312] с опорой на три принципа: верховенство права (англ. «rule of law»), многосторонний и риск-ориентированный подходы (англ. «multi-stakeholder approach», «risk-based approach») — в целях стремления к охраняемому арабскому обществу, интегрированности в глобальную цифровую экономику, комплексным самодостаточным решениям проблем, высокому уровню квалификации и экспертизы, цифровой безопасности. В качестве проблем выделяются имплементация целостного управления кибербезопасности, защита процесса развития (методология управления рисками), обеспечение безопасности коммуникативной инфраструктуры с сохранением свободного потока информации и механизмов обмена ею, защита управления данными, надзор за арабским киберпространством (к чему организации должны стремиться). С точки зрения инициатив отмечается необходимость создания CERT[313], наличия уполномоченного органа и подразделений в сфере ИТ, введение дополнительных обучающих программ в образовательных учреждениях, соблюдение международных стандартов и выработка единого регулирования.

Азия. В рамках АСЕАН важность укрепления кибербезопасности и безопасности ИКТ-экосистемы государств была неоднократно отмечена на ряде встреч и заседаний: встречах Министерского совещания АСЕАН по транснациональной преступности (англ. «AMMTC») в 2013 и 2015 гг., 15-ом заседании Встречи министров телекоммуникаций и информационных технологий стран АСЕАН и связанных с ней совещаниях (англ. «TELMIN»), а также в совместном заявлении Министров обороны стран АСЕАН о развитии оборонного

---

[311] Под Видением (англ. «Vision», араб. «رؤية») понимается обычно национальная стратегия развития государства и отдельных секторов, где указываются цели и прописываются инициативы, в рамках которых реализуются отдельные проекты и программы.

[312] الاستراتيجية العربية الامن السيبراني ٢٠٢٣-٢٠٢٧ [Арабская стратегия по кибербезопасности 2023–2027] // Арабская организация информационно-коммуникационных технологий. URL: https://www.aicto.org/publications/studies/#flipbook-df_6464/1/ (дата обращения: 05.06.2025).

[313] CERT, CSIRT, CIRT зачастую используются как синонимы.

сотрудничества в интересах динамичного сообщества АСЕАН (англ. «ADMM») в 2015 г., на 28-м и 29-м саммитах АСЕАН в 2016 г. Однако ещё раньше (в 2002 г.) была принята Рабочая программа по реализации Плана действий АСЕАН по борьбе с транснациональной преступностью, где уже можно найти не только упоминание киберпреступлений, но и конкретные меры: обмен информацией, проведение исследований типологий преступности, тренды и *modus operandi*, криминализация, укрепление двустороннего и многостороннего уровней для осуществления эффективного сотрудничества, в том числе взаимодействие на уровне правоохранительных органов и разведки, развитие релевантных программ и обучения. Региональный форум АСЕАН регулярно принимал документы в рассматриваемой сфере: Заявление о сотрудничестве в борьбе с кибератаками и неправомерным использованием киберпространства террористами от 28.07.2006 (Кулуа-Лумпур, Малайзия), Заявление министров иностранных дел о сотрудничестве в обеспечении кибербезопасности от 12.07.2012 (Пном Пен, Камбоджа) [314] и Рабочий план по безопасности ИКТ и их использовании от 07.05.2015 (принят и утверждён 06.08.2015, Кулуа-Лумпур)[315].

В рамках АСЕАН борьба именно с киберпреступностью ведётся в первую очередь в рамках программ по предупреждению транснациональной преступности, о чём было принято решение во время 3-й Встречи АММТС (Сингапур, 11.10.2001): в План действий по борьбе с транснациональной преступностью (Янгон, 23.06.1999) были внесены соответствующие изменения. Примером также может служить Программа работы Совещания высших должностных лиц по транснациональной преступности (англ. «SOMTC») 2013–2015 гг., которая согласно совместному

[314] ASEAN Regional forum statement by the ministers of foreign affairs on cooperation in ensuring cyber security // ASEAN Regional forum. URL: https://aseanregionalforum.asean.org/wp-content/uploads/2019/01/ARF-Statement-on-Cooperation-in-Ensuring-Cyber-Security.pdf (accessed 27.04.2025).

[315] SEAN REGIONAL FORUM WORK PLAN ON SECURITY OF AND IN THE USE OF INFORMATION AND COMMUNICATIONS TECHNOLOGIES (ICTs) // ASEAN Regional forum. URL: https://aseanregionalforum.asean.org/wp-content/uploads/2018/07/ARF-Work-Plan-on-Security-of-and-in-the-Use-of-Information-and-Communications-Technologies.pdf (accessed 27.04.2025).

коммюнике 47-й Встречи министров иностранных дел АСЕАН (Нейпьидо, 08.08.2014)[316] регулирует нетрадиционные вопросы безопасности.

На 7-м Совещании SOMTC (Вьентьян, 26–27.06.2007) была принята общая рамочная программа по наращиванию потенциала АСЕАН в области борьбы с киберпреступностью в поддержку глобальной борьбы с киберпреступностью.

13.11.2017 в Маниле (Филиппины) AMMTC приняло Декларацию АСЕАН по предупреждению и борьбе с киберпреступностью, содержавшую 10 пунктов: гармонизация законодательства, присоединение к существующим международно-правовым документам, развитие национальных планов действий, укрепление и усиление международного сотрудничества в сфере технической экспертизы, обмен опытом и лучшими практиками, оказание образовательной, профессиональной, административной и технической помощи, повышение осведомлённости, развитие диалога с партнёрами (ЕВРОПОЛ, ИНТЕРПОЛ, АСЕАНАПОЛ), мониторинг, участие в Глобальном инновационном комплексе Интерпола (англ. «IGCI»)[317].

14.01.2011 был принят Генеральный план АСЕАН в сфере ИКТ 2015 (англ. «AIM2015») [318] , в котором напрямую не упоминались меры по борьбе с киберпреступностью, но затрагивались вопросы экономической трансформации (создание благоприятной бизнес-среды для привлечения и продвижения торговли, инвестиций и предпринимательства в секторе ИКТ), расширение прав и вовлечение населения (повышение качества жизни посредством доступных и справедливых ИКТ), инновации (содействие созданию творческого, инновационного и зеленого сектора ИКТ), развитие инфраструктуры (для поддержки предоставления услуг всем сообществам АСЕАН); развитие человеческих ресурсов (компетентных и квалифицированных кадров для поддержки роста сектора ИКТ и содействия

---

[316] Joint Communiqué 47th ASEAN Foreign Ministers' Meeting 8 August 2014 Nay Pyi Taw, Myanmar // ASEAN. URL: https://asean.org/wp-content/uploads/2012/05/Joint-Communique-of-47th-AMM.pdf (accessed 27.04.2025).

[317] ASEAN Declaration to prevent and combat cybercrime. Manila, the Philippines, 13 November 2017 // ASEAN. URL: https://asean.org/wp-content/uploads/2017/11/ASEAN-Declaration-to-Combat-Cybercrime.pdf (accessed 27.04.2025).

[318] AIM2015 // ASEAN. URL: https://asean.org/wp-content/uploads/images/2012/Economic/TELMIN/ASEAN%20ICT%20Masterplan%202015.pdf (accessed 27.04.2025).

преобразованию других секторов экономики), преодоления цифрового разрыва (преодоление пробелов для содействия более широкому внедрению ИКТ). Далее был принят новый Генеральный план АСЕАН в сфере ИКТ 2020 (англ. «AIM2020»)[319] TELMIN по трём направлениям: реагирование на инциденты в области кибербезопасности; политика и координация деятельности CERT; наращивание потенциала в области кибербезопасности в гражданском киберпространстве с опорой на 8 стратегических целей (экономическая интеграция и трансформация, интеграция и расширения прав и возможностей людей с помощью ИКТ, инновации, развитие инфраструктуры ИКТ, развитие человеческого капитала, ИКТ на едином рынке, новые медиа и контент, информационная безопасность и уверенность) — порученных Встрече старших должностных лиц по телекоммуникациям и информационным технологиям (англ. «TELSOM»). Отметим, что киберпреступность, киберзащита и кибердипломатия не входили в мандат TELMIN, поэтому данные вопросы исключались. Аналогичное можно говорить и о Генеральном плане АСЕАН в сфере ИКТ 2025 (англ. «ADM2025»), охватывающем цифровые инфраструктуру, трансформацию, политику, регулирование и стандарты, устойчивость, доверие и безопасность, коллаборацию и сотрудничество[320].

Сопоставляя стратегии АСЕАН по сотрудничеству в сфере кибербезопасности 2017–2020 гг. и 2021–2025 гг., расширен перечень инициатив, однако опора в основном на Генеральные планы АСЕАН в сфере ИКТ (см. Приложение № 5). Помимо этого, разработан ряд рамочных соглашений по защите персональных данных (2016 г.), международному мобильному роумингу (2017 г.), управлению цифровыми данными (2018 г.), обязательствам по обслуживанию следующего поколения (2019 г.), управлению данными (2021 г.), развитию роста цифровых стартапов; руководств по защите КИИ (2016 г.), повышению устойчивости и восстановлению подводных кабелей (2019 г.), развитию

---

[319] AIM2020 // ASEAN. URL: https://asean.org/wp-content/uploads/images/2015/November/ICT/15b%20--%20AIM%202020_Publication_Final.pdf (accessed 27.04.2025).

[320] AIM2025 // ASEAN. URL: https://asean.org/book/asean-digital-masterplan-2025/ (accessed 27.04.2025).

экосистемы 5G, по управлению и этике ИИ (с дополнениями), анонимизации данных, системе управления данными и механизму трансграничной передачи данных и отдельным договорным оговоркам для различных регионов (e.g., ЕС и ЛА)[321].

Африка. В рамках Повестки 2063 Африканского Союза Группой экспертов по кибербезопасности разрабатывается континентальная стратегия кибербезопасности. На сегодняшний день достигнут успех в согласовании руководящих документов в отдельных областях: цифровая трансформация 2020–2030 гг. от 18.05.2020[322], Политика и регулирующая инициатива для цифровой Африки (англ. «PIDA»), План приоритетных действий в сфере ИКТ к PIDA, континентальная стратегия по ИИ от 07.2024[323], Политика АС по расширению прав и безопасности детей в Интернете от 21.05.2024, Региональная программа цифровой интеграции Западной Африки (англ. «WARDIP») от 20.03.2024, Платформа совместимости АС для цифрового идентификатора от 11.12.2023, Рамочная программа АС по политике данных от 28.07.2022, Стратегия: Разработка согласованной нормативно-правовой базы для «AfSEM» от 18.06.2021[324]. В них особо подчеркивается рост киберпреступности, возможность использования Интернета вещей для её предупреждения.

Начиная с 2019 года, Комиссия Экономического сообщества западноафриканских государств в партнерстве с Европейским союзом инициировала Западноафриканские меры реагирования на кибербезопасность и борьбу с киберпреступностью (англ. «OCWAR-C») и приняла Региональную стратегию кибербезопасности и киберпреступности в январе 2021 г.[325]. АФРИПОЛ

---

[321] Key Documents // ASEAN. URL: https://asean.org/our-communities/economic-community/asean-digital-sector/ (accessed 03.05.2025).

[322] THE DIGITAL TRANSFORMATION STRATEGY FOR AFRICA (2020-2030) // AU. URL: https://au.int/sites/default/files/documents/38507-doc-dts-english.pdf (accessed 04.05.2025).

[323] Continental AI Strategy // AU. URL: https://au.int/sites/default/files/documents/44004-doc-EN-_Continental_AI_Strategy_July_2024.pdf (accessed 04.05.2025).

[324] Latest Documents // AU. URL: https://au.int/documents/69 (accessed 04.05.2025).

[325] Ajijola A.-H., Allen Nate D.F. African Lessons in Cyber Strategy // Africa Center for strategic studies. 08.03.2022. URL: https://africacenter.org/spotlight/african-lessons-in-cyber-strategy/ (accessed 04.05.2025).

разработал Стратегию борьбы с киберпреступностью 2020-2024 гг.[326], которая направлена на улучшение координации с EAPCCO, CAPCCO, WAPCCO, SARPCCO, Интерполом (в рамках взаимодействия I24/7 и AFSECOM), Европолом, Америполом, АСЕАНАПОЛом, МСЭ, Европейским полицейским колледжем (англ. «CEPOL»), УНП ООН, Корпорацией по управлению доменными именами и IP-адресами и охватывает 4 приоритетных направления: усиление кибер-команды для ресурсов и механизмов по сбору доказательств, необходимых для цифровых расследований, наращивание потенциала посредством тренингов, развитие гармоничного законодательства для целей международного сотрудничества и обеспечение оценки рисков.

Национальный уровень. В то время как в Видениях арабских стран и доктринах безопасности других государств Глобального Юга уделяется внимание лишь общим вопросам цифровизации, на уровне отдельных уполномоченных органов (министерств, комиссий или управлений) утверждены национальные стратегии кибербезопасности (см. Приложение № 5)[327].

Необходимо учитывать государственное устройство рассматриваемых стран, особенно это касается федераций. В то время как в ФДРЭ принят только один централизованный документ, в ОАЭ в дополнение к федеральному уровню в субъекте (эмират Дубай) разработан также отдельный документ[328]. Ещё одним

---

[326] AFRIPOL cybercrime strategy // Council of Europe. URL: https://rm.coe.int/afripol-strategy-on-cybercrime-v01-en/1680a30050 (accessed 04.05.2025).

[327] الاستراتيجية الوطنية للأمن السيبراني [Национальная стратегия кибербезопасности] // Национальное управление кибербезопасности KCA. URL: https://nca.gov.sa/strategic (дата обращения: 25.03.2025); Qatar National Cyber Security Strategy. May 2014 // The George Washington University. URL: https://nsarchive.gwu.edu/sites/default/files/documents/3903662/Qatari-Government-Qatar-National-Cyber-Security.pdf (дата обращения: 25.03.2025); الاستراتيجية الوطنية للأمن السيبراني [Национальная стратегия кибербезопасности] // Национальный центр кибербезопасности Королевства Бахрейн. URL: https://www.ncsc.gov.bh/ar/national-strategy.html (дата обращения: 11.03.2025); الاستراتيجية الوطنية للأمن السيبراني [Национальная стратегия кибербезопасности] // Управление по регулированию телекоммуникаций и цифрового государства ОАЭ. URL: https://tdra.gov.ae/ar/national-cybersecurity-strategy (дата обращения: 25.03.2025).

[328] the Dubai Cyber Security Strategy — Updated // ОАЭ. URL: https://u.ae/en/about-the-uae/strategies-initiatives-and-awards/strategies-plans-and-visions/government-services-and-digital-transformation/dubai-cyber-security-strategy (дата обращения: 25.03.2025); Shires J., Hassib B. Cybersecurity in the GCC: From Economic Development to Geopolitical Controversy // Middle East Policy. 2022. № 29 (1). P. 90–103. С. 93.

примером служит Республика Индия: Политика штата Махараштры в области облачных вычислений 2018 года, Политика электронного управления штата Махараштры, Политика информационной безопасности штата Уттар-Прадеш, Политика кибербезопасности штата Ассам на 2020 год, Политика кибербезопасности штата Теланган 2016 года, Рамочная программа по внедрению облачных вычислений в штате Мадхья-Прадеш 2022 года[329].

На первый взгляд, из стран Аравийской зоны только в Султанате Оман не обнаружено описанной концепции, хотя соответствующих инициатив, руководств и политик есть предостаточно. Возможно, это объясняется тем, что ответственному органу изначально было поручено разработать закон о борьбе с преступлениями в области информационных технологий. Да и первым шагом в арабских странах зачастую была именно криминализация новых видов деяний, что в свою очередь относится к уголовно-правовым средствам обеспечения кибербезопасности. Тем не менее на самом деле Стратегия цифрового Омана была принята ещё в 2003 г. (обновлена в 2010 г.). Она прошла долгий путь модернизации и расширения: в 2014 г. — Национальная стратегия широкополосной связи, в 2017 г. — Стратегия цифрового Омана 2030 (англ. «eOman»), в 2020 г. — Национальная программа цифровой экономики, Государственная программа цифровой трансформации, в 2022 г. — Национальная стратегия данных, Национальная программа искусственного интеллекта и передовых технологий[330]. В СО также имеется циркуляр Министерства транспорта, связи и информационных технологий № 11/2025 от 09.04.2025 «Общая политика безопасного и этического использования систем искусственного интеллекта», применимый как к государственному, так и к

---

[329] Assessing India’s Cybersecurity Regulations in a Dynamic Environment // DSCI. URL: https://www.dsci.in/files/content/knowledge-centre/2024/Assessing-India-Cybersecurity-Regulations-DSCI-SAP.pdf (accessed 24.05.2025).

[330] البرنامج الوطني للاقتصاد الرقمي [Национальная программа цифровой экономики] // Министерство транспорта, связи и информационных технологий Султаната Оман. URL: https://ita.gov.om/ITAPortal_AR/Our_Projects/Our_Projects_List.aspx?svc=657&NID=170001&Odt=37 (дата обращения: 25.03.2025); البرنامج الوطني للذكاء الاصطناعي والتقنيات المتقدمة [Национальная программа искусственного интеллекта и передовых технологий] // URL: https://mtcit.gov.om/ITAPortal_AR/Our_Projects/Our_Projects_List.aspx?svc=657&NID=170035&Odt=37 (дата обращения: 25.03.2025).

частному секторам, которые разрабатывают или используют системы ИИ, включая сбор данных, проектирование, обучение, эксплуатацию и оценку[331].

Любопытно, что хотя в КСА позднее других стран Персидского залива была принята концепция кибербезопасности, ещё в 2012 г. Наиф бин Ахмед бин Абдулазиз Ас-Сауд до кибератаки на государственную компанию «Saudi Aramco» в своей работе «Саудовский взгляд на стратегии кибербезопасности, экстраполированный на западный опыт» рассматривал необходимость принять соответствующий документ, опираясь на американский опыт[332].

Хронологически первые документы появились в 2010-х годах и по прошествии примерно 7–10 лет были обновлены[333]. Например, в Республике Индия впервые принята национальная политика кибербезопасности в 2013 г. и обновлена в 2020 г. Количество направлений увеличилось с 15 до 21. В Государстве Катар первая стратегия была разработана в 2014 г. Недавно, в 2024 г., была принята новая — до 2030 г. Документ стал носить более комплексный характер. Пять общих направлений: защита КИИ, реагирование на киберинциденты и атаки, разрешение проблем и восстановление после них посредством своевременного обмена информацией, сотрудничества и активных действий, совершенствование нормативно-правовой базы для развития безопасного и динамичного киберпространства, развитие культуры киберэтики, развитие мощностей — обросли чётко сформулированными целями, структурированными задачами и проектами.

Отметим, что по общему правилу разработкой и принятием соответствующих политик занимались специализированные органы. Принятие доктрины высшим должностным лицом является скорее исключением из правил в странах

---

331 وزارة النقل والاتصالات وتقنية المعلومات: تعميم رقم ١١ / ٢٠٢٥ السياسة العامة للاستخدام الآمن والأخلاقي لأنظمة الذكاء الاصطناعي أبريل ٢٠٢٥م [Ministry Of Transport, Communications, And Information Technology: Circular 11/2025 The Public Policy For The Safe And Ethical Use Of Artificial Intelligence Systems April 2025] // Qanoon. URL: https://qanoon.om/p/2025/mtcit20259901/ (accessed 20.05.2025).

332 Al-Saud N. B. A. A Saudi Outlook for Cybersecurity Strategies Extrapolated from Western Experience // Joint Force Quarterly. 2012. № 64. P. 75–81.

333 Цыплакова А.Д. Борьба с киберпреступностью в странах Глобального Юга: сравнительно-правовое исследование // Пролог: журнал о праве. 2025. № 1. С. 99–110.

Глобального Юга — Стратегия цифрового Омана 2003 г. и Регулирование Президента Республики Индонезия № 7 от 20.07.2023 «О национальной стратегии кибербезопасности и менеджменте киберкризисами»[334]. Первая прошла долгий путь модернизации и расширения: обновлена в 2010 г., в 2014 г. — Национальная стратегия широкополосной связи, в 2017 г. — Стратегия цифрового Омана 2030 (англ. «eOman»), в 2020 г. — Национальная программа цифровой экономики, Государственная программа цифровой трансформации, в 2022 г. — Национальная стратегия данных и Национальная программа искусственного интеллекта и передовых технологий[335].

Несмотря на отсутствие в ИРИ национальной стратегии по обеспечению кибербезопасности, отметим отдельные инициативы: Генеральный план и архитектура по обеспечению национальной информационной сети в области снижения темпов роста киберпреступности и содействия укреплению здоровья и сокращения вредоносного и преступного контента в публичном пространстве (15.09.2020)[336], документ «Предотвращение и борьба с азартными играми в киберпространстве» (11.10.2022), утверждённые Высшим советом по киберпространству страны[337]; Национальный документ ИРИ по ИИ, утверждённый Верховным Советом по культурной революции от 18.06.2024[338].

---

[334] Regulation of the President of the Republic of Indonesia Number 47 Of 2023 On National Cyber Security Strategy And Cyber Crisis Management // Peraturan. URL: https://peraturan.go.id/files2/perpres-no-47-tahun-2023_terjemah.pdf (accessed 05.04.2025).

[335] البرنامج الوطني للاقتصاد الرقمي [Национальная программа цифровой экономики] // Министерство транспорта, связи и информационных технологий Султаната Оман. URL: https://ita.gov.om/ITAPortal_AR/Our_Projects/Our_Projects_List.aspx?svc=657&NID=170001&Odt=37 (дата обращения: 05.04.2025); البرنامج الوطني للذكاء الاصطناعي والتقنيات المتقدمة [Национальная программа искусственного интеллекта и передовых технологий] // URL: https://mtcit.gov.om/ITAPortal_AR/Our_Projects/Our_Projects_List.aspx?svc=657&NID=170035&Odt=37 (дата обращения: 05.04.2025).

[336] طرح کلان ومعماری شبکه ملی اطلاعات [Генеральный план и архитектура национальной информационной сети] // Законодательная база ИРИ. URL: https://davoudabadi.ir/page/60451726 (дата обращения: 04.05.2025).

[337] پیشگیری ومقابله با قمار در فضای مجازی [Предотвращение и борьба с азартными играми в киберпространстве] // Законодательная база ИРИ. URL: https://davoudabadi.ir/page/1790426 (дата обращения: 04.05.2025).

[338] سند ملی هوش مصنوعی جمهوری اسلامی ایران [Национальный документ Исламской Республики Иран по искусственному интеллекту] // Законодательная база ИРИ. URL: https://davoudabadi.ir/page/0392571/سند-ملی-هوش-مصنوعی-جمهوری-اسلامی-ایران (дата обращения: 04.05.2025).

В КНР особое внимание уделяется кибербезопасности, поскольку ещё в 2014 г. было объявлено, что страна станет «киберсилой»; в 2016 г. была принята стратегия кибербезопасности, а годом позже — международная стратегия по сотрудничеству в киберпространстве (обновлена в 2024 г.)[339].

Помимо национальной стратегии по кибербезопасности, также параллельно разрабатываются иные руководящие документы в смежных областях в странах Глобального Юга: искусственного интеллекта, электронного правительства, цифровой аутентификации и предоставления государственных услуг, Интернета вещей, Блокчейна и электронного документооборота.

Первые три инициативы реализованы, например, компетентным министерством Катара в 2019–2024 гг.[340]. С опорой на исламскую философию отмечаются стремления к совершенствованию различных секторов с помощью ИИ (англ. «AI+X», араб. «اعتماد الذكاء الاصطناعي»). В период 2017–2025 годов в ОАЭ было обновлено ряд положений в сфере электронной безопасности путём принятия новых программных документов: стратегия ОАЭ в области ИИ 2031 от 10.2017, национальная стратегия передовых инноваций от 02.2018, стратегия электронного участия от 09.06.2023, стратегия цифровой экономики от 04.2022, национальная стратегия электронного правительства 2025 г., национальная политика качества цифровой жизни, стратегия государственных услуг 2025 г.[341].

---

[339] Creemrs R. The Chinese Conception of Cybersecurity: A Conceptual, Institutional and Regulatory Genealogy // Journal of Contemporary China. 2023. № 33 (146). P. 173–188.

[340] استا تيجية قطر الوطنية في نجال الذكاء الاصطناعي [Стратегия Государства Катар в области искусственного интеллекта] // Министерство связи и информационных технологий Государства Катар. URL: https://mcit.gov.qa/sites/default/files/strtyjy_qtr_lwtny_fy_mjl_ldhk_lstny.pdf (дата обращения: 25.03.2025) и استراتيجية الحكومة الإلكترونية لدولة قتر ٢٠٢٠[Стратегия электронного правительства Государства Катар 2020] // Министерство связи и информационных технологий Государства Катар. URL: https://mcit.gov.qa/sites/default/files/qatar-e-government-2020-strategy-ar_0.pdf (дата обращения: 25.03.2025).

[341] Digital Participation Strategy // U.ae. URL: https://u.ae/en/about-the-uae/digital-uae/digital-inclusion/national-digital-participation-strategy (accessed 20.03.2025); National Strategy for Advanced Innovation // U.ae. URL: https://u.ae/en/about-the-uae/strategies-initiatives-and-awards/strategies-plans-and-visions/innovation-and-future-shaping/national-strategy-for-advanced-innovation (accessed 25.03.2025), National Policy for Quality of Digital Life // U.ae. URL: https://u.ae/en/about-the-uae/strategies-initiatives-and-awards/policies/government-services-and-digital-transformation/national-policy-for-quality-of-digital-life (accessed 25.03.2025); استراتيجية الإمارات الوطنية للذكاء الاصطناعي [Национальная стратегия ОАЭ по искусственному интеллекту 2031] // Министерство ОАЭ по искусственному интеллекту, цифровой экономике и удалённой работе.

На уровне субъектов лидерство по охвату областей занимает Дубай: автономная транспортная стратегия, стратегия 3D-печати, стратегия данных, стратегия кибербезопасности, Блокчейн-стратегия, стратегия Интернета вещей, стратегия электронного документооборота (дословно с араб. «للمعاملات اللاورقية» безбумажная), стратегия электронной коммерции, стратегия умного Дубай 2021, стратегия метавселенной[342]. В Абу-Даби — концепция электронной трансформации и стратегия цифрового правительства 2025–2027 от 01.01.2025[343]; в Аджмане — генеральный цифровой план 2017–2022, соответственно[344].

Сходные стратегии, руководства, политики, модели есть и в Султанате Оман, причём список может быть расширен: рамки информационной безопасности, политика «Cloud First», платформа непрерывности ИТ-услуг, национальная стратегия широкого диапазона, основные рекомендации по контролю безопасности, рамки облачного управления, руководство по управлению кибербезопасности, карта классификации безопасности данных и информационных систем, политика

URL: https://ai.gov.ae/wp-content/uploads/2021/07/UAE-National-Strategy-for-Artificial-Intelligence-2031-AR.pdf (дата обращения: 25.03.2025).

[342] Smart Dubai 2021 Strategy // U.ae. URL: https://u.ae/en/about-the-uae/strategies-initiatives-and-awards/strategies-plans-and-visions/strategies-plans-and-visions-untill-2021/smart-dubai-2021-strategy (accessed 20.03.2025); Dubai Data Strategy // U.ae. URL: https://u.ae/en/about-the-uae/strategies-initiatives-and-awards/strategies-plans-and-visions/government-services-and-digital-transformation/dubai-data-strategy (accessed 25.03.2025); Dubai Autonomous Transportation Strategy // U.ae. URL: https://u.ae/en/about-the-uae/strategies-initiatives-and-awards/strategies-plans-and-visions/transport-and-infrastructure/dubai-autonomous-transportation-strategy (accessed 25.03.2025); Dubai 3D Printing Strategy // U.ae. URL: https://u.ae/en/about-the-uae/strategies-initiatives-and-awards/strategies-plans-and-visions/industry-science-and-technology/dubai-3d-printing-strategy (accessed 25.03.2025); Dubai Blockchain Strategy // Digital Dubai. URL: https://www.digitaldubai.ae/initiatives/blockchain (accessed 20.03.2025); Dubai Internet of Things Strategy // U.ae. URL: https://u.ae/en/about-the-uae/strategies-initiatives-and-awards/strategies-plans-and-visions/strategies-plans-and-visions-untill-2021/dubai-internet-of-things-strategy (accessed 25.03.2025); Dubai Paperless Strategy // Digital Dubai. URL: https://www.digitaldubai.ae/initiatives/paperless (accessed 25.03.2025); Dubai eCommerce strategy // U.ae. URL: https://u.ae/en/about-the-uae/strategies-initiatives-and-awards/strategies-plans-and-visions/government-services-and-digital-transformation/dubai-e-commerce-strategy (accessed 25.03.2025).

[343] Abu Dhabi Government Digital Strategy 2025-2027 // Abu Dhabi Media Office. URL: https://www.mediaoffice.abudhabi/en/topic/abu-dhabi-government-digital-strategy-2025-2027/ (accessed 25.03.2025).

[344] The UAE Digital Government Strategy 2025 // ОАЭ. URL: https://u.ae/en/about-the-uae/strategies-initiatives-and-awards/strategies-plans-and-visions/government-services-and-digital-transformation/uae-national-digital-government-strategy (дата обращения: 25.03.2025).

удалённого доступа к ИКТ, политика электронного голосования, правительственная политика в отношении открытых данных, политика в социальных сетях, рамки управления ИТ-рисками, эталонные модели, стандарты проектирования веб-сайтов и государственных порталов электронных услуг, руководство по защите детей в Интернете, стандарты безопасности базы данных и хартия управления ИТ, а также документы по управлению проектами[345].

Что касается арабских стран в целом (в частности, КСА и Бахрейна), то можно выделить технические руководства и стандарты, в том числе касающиеся регистрации доменных имён, оказания услуг связи, онлайн-банкинга, пользовательского интерфейса, контроля уменьшения спама, использования социальных сетей, применения мобильных телефонов, программного обеспечения мобильных телефонов и криптовалюты[346].

Как для частного сектора, так и для учреждений КИИ уполномоченные органы и GCC-CERT разрабатывают стандарты (см. пример в Приложении № 6), процедуры по прохождению сертификации и лицензирования, признанию органа оценки рисков и руководству по системе управления качества, контролю безопасности, классификации безопасности данных и информационных систем, свободному и открытому ПО, регулированию конфиденциальности данных пользователей и баз данных, правила и требования к поставщикам услуг в сфере IT[347]. Иногда они упорядочены и собраны на одном сервисе по типу дополнения к матрице «MITRE ATT & CK» от Bh-CERT.

---

[345] Policies, strategies and guidelines // Omanuna. URL: https://oman.om/en/policies-strategies-and-guidlines (accessed 25.03.2025).

[346] الإطار القانوني الاسترشادي [Руководящая правовая база] // Портал Совета сотрудничества арабских государств Персидского залива. URL: http://www.gcc-egov.org/web/guest/laws;jsessionid=B5AC15C1BAC7D86B98BCC5A668E5D826 (дата обращения: 25.03.2025).

[347] Организация по стандартизации GCC перечисляет арабские версии стандартов кибербезопасности ISO 27001, опубликованные в 2009 и 2015 годах соответственно. Примечательно, что в ОАЭ опубликована собственные стандарты обеспечения информации (IAS), основанные на версиях ISO 27001 2005, 2013 года, и основу кибербезопасности NIST 2014 США. В качестве примеров также см. подробней الضوابط والإرشادات [Контроль и руководящие принципы] // Национальное управление кибербезопасности КСА. URL: https://nca.gov.sa/legislation (дата обращения: 16.04.2025); الأمن السيبراني في قطاع الاتصالات والفضاء والتقنية [Кибербезопасность в телекоммуникационном, космическом и технологическом секторе] //

При этом ни на региональном, ни на национальном уровнях нет документов, связанных с квантовыми технологиями [348]. С точки зрения противодействия киберпреступности это можно рассматривать в качестве пробела, поскольку квантовые компьютеры представляют уже вполне реальную угрозу и орудие для хакерской атаки (взлома алгоритмов шифрования, используемых в банковской сфере и Блокчейне)[349].

В арабоязычной юридической литературе отмечается значительное отсутствие исполнительных правил и нормативных инструментов для правоохранительных органов в части цифровой криминалистики, что осложняется недостаточной квалифицированностью должностных лиц [350]. Отсутствие регулирования объясняется широкой дискрецией при проведении расследований. Более того, встречаются исследования, в которых алгоритм расследования электронных преступлений совпадает с традиционным; указывается

Комиссия по связи, космосу и технологиям КСА. URL: https://www.cst.gov.sa/ar/RulesandSystems/CyberSecurity/Pages/default.aspx (дата обращения: 16.04.2025); المحافظة على خصوصية البيانات الشخصية [Поддержание конфиденциальности персональных данных] // Комиссия по связи, космосу и технологиям КСА. URL: https://www.cst.gov.sa/ar/RulesandSystems/privacy/Pages/default.aspx (дата обращения: 16.04.2025); حوكمة تقنية المعلومات [Управление информационными технологиями] // Министерство транспорта, коммуникаций и информационных технологий Султаната Оман. URL: https://www.ita.gov.om/ITAPortal_AR/Pages/Page.aspx?NID=2187&PID=6706&LID=247 (дата обращения: 13.04.2025); المعايير والسياسات [Стандарты и политика] // Центр электронной безопасности в Дубай. URL: https://www.desc.gov.ae/ar/regulations-ar/standards-policies-ar/ (дата обращения: 17.04.2025).

[348] Отметим, что передовыми в этой сфере являются РФ и ЕС. См. Распоряжение Правительства РФ от 11 июля 2023 г. N 1856-р «Об утверждении Концепции регулирования отрасли квантовых коммуникаций в РФ до 2030 г.» // Собрание законодательства Российской Федерации. 2023. № 30. Ст. 5712, Quantum Europe Strategy // European Union. URL: https://digital-strategy.ec.europa.eu/en/library/quantum-europe-strategy (accessed 07.07.2025).

[349] Katte S. Scientists breach cryptographic algorithms with quantum computer: SCMP // Coin telegraph. 14.10.2024. URL: https://cointelegraph.com/news/scientists-breach-crypto-algorithms-quantum-computer-report (accessed 06.06.2025).

[350] ليلى الجنابي. فعالية القوانين الوطنية والدولية في مكافحة الجرائم السيبرانية [Лайла Аль-Джанаби. Эффективность национального и международного права в борьбе с киберпреступлениями] // Центр светских работ и исследований в арабском мире. URL: https://www.ssrcaw.org/ar/show.art.asp?aid=571423 (дата обращения: 25.03.2025); نضال أدلبي، بحث بعنوان تطوير وتنسيق التشريعات السيبرانية في المنطقة العربية ومواجهة الجرائم السيبرانية، الأمم المتحدة ، الإسكوا،نقل بتصرف، ص 14- 18 [Нидаль Эдби. Разработка и гармонизация киберзаконодательства в арабском регионе и противостояние киберпреступности. ЭСКЗА ООН. С. 14–18], Maarouf K. Procedural Problems Facing a Criminal Investigator in Cybercrimes // Arab Journal of Forensic Sciences and Forensic Medicine. 2022. № 4 (2). P. 158–166.

необходимость знания основ работы компьютеров и сетей [351] . Одним из фундаментальных является Руководство Арабского университета наук безопасности им. принца Наифа бин Абдель Азиза 2024 г. Тем не менее данная проблематика характерна для не только стран Ближнего Востока и Северной Африки, но и африканского региона в целом.

Что касается **Азии**, то отметим Руководство по расследованию киберпреступлений, разработанное Советом по цифровой безопасности Индии с участием правоохранительных органов в 2011 г. [352] . Впоследствии, после учреждения Центра по исследованию и обучению расследований киберпреступлений в 2019 г. указанной некоммерческой организацией, полицейским департаментом штата Карнатака и НКО «Infosys Foundation» активным образом развивается выпуск руководств по узконаправленным темам: Даркнет и глубокий Интернет (07.02.2022), третье издание указанного руководства в двух томах (19.05.2023), достижения в области противодействия расследованиям киберпреступлений (19.09.2023), дроны (11.03.2024), избыточный массив независимых (самостоятельных) дисков (англ. «RAID») (18.10.2024), айфоны (29.01.2025)[353].

§ 2. Институциональные механизмы противодействия киберпреступлениям в отдельных странах Глобального Юга

На **региональном** уровне отметим совещания отдельных министров, рабочих групп и компьютерные группы реагирования на чрезвычайные ситуации (англ. «CERT») на уровне ССАГПЗ (англ. «GCC-CERT»), ОИС (англ. «OIC-CERT»), АСЕАН (англ. «ACERT»), АТР (англ. «APCERT»), АС (англ. «AfricaCERT»).

---

[351] Например, см. подробней خالد علي نازل الشعار. التحقيق الجنائي في الجرائم الإلكترونية [Аш-Шаар Халид Али Назал. Уголовное расследование электронных преступлений] // Журнал юридических и экономических исследований. 2022. № 12 (79). С. 133–183.

[352] Cyber Crime Investigation Manual. DSCI, 2011. 137 p. URL: https://jhpolice.gov.in/sites/default/files/documents-reports/jhpolice_cyber_crime_investigation_manual.pdf (accessed 08.04.2025).

[353] Center For Cybercrime Investigation Training & Research // DSCI. URL: https://www.dsci.in/content/ccitr (accessed 08.04.2025).

В рамках ССАГПЗ отсутствует специализированные бюро (араб. «مكتب»), союз (араб. «اتحاد») или служба (араб. «جهاز») по кибербезопасности[354]. Ещё в 2011 г. данный вопрос поднимался в арабоязычной доктрине[355]. На сегодняшний день действует комитет по кибербезопасности Генерального секретариата Совета (араб. «جنة الأمن السيبراني بدول مجلس التعاون»), первое заседание которого состоялось совместно с полицейской службой Совета сотрудничества арабских государств Персидского залива (араб. «جهاز الشرطة الخليجية», англ. «GCCPol») 10.02.2017, исполнительный комитет электронного правительства и комитет почтовых и телекоммуникационных агентств, в заседаниях которого участвуют министерства информационных технологий и коммуникаций, а также комитет министров по кибербезопасности, который провёл первое заседание 23.10.2022[356].

До недавнего времени подобное относилось отчасти и к Лиге арабских государств. В 2023 г. КСА на 160-ой сессии было предложено создание Совета арабских министров по кибербезопасности. 24.12.2024 была проведена их первая встреча. До того были учреждены более широкие специализированные органы и организации по типу Арабская организация ИКТ (13.02.2002), Арабская организация спутниковой связи (14.04.1976), Арабское бюро по вопросам

---

354 Подобная практика активно реализуется в рамках ОИС. См. подробней о рекомендациях конференции по кибербезопасности الخليجي للأمن السيبراني يوصي باستراتيجية موحدة لمتابعة الجرائم الإلكترونية [«Gulf Cybersecurity» рекомендует единую стратегию по борьбе с киберпреступностью] // Aljarida. 15.03.2023. URL: https://www.aljarida.com/article/17840 (дата обращения: 25.03.2025).

355 ريتشارد كلارك, روبرت نيك. حماية الفضاء الإلكتروني في دول مجلس التعاون لدول الخليج العربية [Нир Р., Кларк Р. Защита электронного пространства в странах Совета сотрудничества стран Арабского залива]. Emirates Center for Strategic Studies and Research, 2011. 55 с. URL: https://www.ecssr.ae/wp-content/uploads/2019/01/ELS_AR_140.pdf (дата обращения: 25.03.2025). С. 33.

356 وزارة التقنية والاتصالات تشارك في اجتماع اللجنة التنفيذية للحكومة الإلكترونية ولجنة وكلاء البريد والاتصالات بدول مجلس التعاون لدول الخليج العربية [Министерство технологий и коммуникаций участвует в заседании Исполнительного комитета электронного правительства и комитета почтовых и телекоммуникационных агентств в государствах Персидского залива] // Oman News Agency. URL: https://omannews.gov.om/topics/ar/112/show/378724 (дата обращения: 02.04.2025); انعقاد أول اجتماع للجنة الخليجية للأمن السيبراني بالإمارات [Первое заседание Комитета по кибербезопасности Персидского залива в ОАЭ] // Alkhaleej. URL: https://alkhaleejonline.net/-علوم-وتكنولوجيا/انعقاد-أول-خلال انعقاد الاجتماع الأول للجنة (дата обращения: 25.03.2025); اجتماع-للجنة-الخليجية-للأمن-السيبراني-بالإمارات الوزارية للأمن السيبراني بدول مجلس التعاون ... إطلاق التمرين الخليجي الأول للأمن السيبراني [Во время первого заседания Министерского комитета по кибербезопасности в странах Персидского залива ... Запуск первых учений по кибербезопасности в Персидском заливе] // Генеральный секретариат ССАГПЗ. URL: https://www.gcc-sg.org/ar-sa/MediaCenter/NewsCooperation/News/Pages/news2022-10-23-4.aspx (дата обращения: 25.03.2025).

безопасности и СМИ AIMC, а также Совет арабских министров по коммуникации и информации (фактически цели в Уставе, утверждённом решением № 6142-д.е.(118)-3-ж. от 05.09.2002, касаются вопросов СМИ).

Что касается АСЕАН, то отметим следующее: с 2001 г. координирующим органом выступал TELMIN, который был преобразован во Встречу цифровых министров АСЕАН (англ. «ADGMIN») в 2019 г., а в качестве вспомогательного — TELSOM, переименованный в указанный год во Встречу цифровых руководящих должностных лиц АСЕАН (англ. «ADGSOM»). При ADGSOM существует ряд органов для реализации отдельных инициатив: Совет по сетевой безопасности (с 2012 г. на основании AIM2015), рабочая группа по управлению цифровыми данными (с 2018 г. для реализации соответствующей рамочной программы), рабочая группа для формата АСЕАН+1 (Китай, Япония, Корея, Индия, ЕС, США и Международный союз электросвязи). В качестве консультативного органа выступает созданный ещё в 1995 г. Совет регуляторов телекоммуникаций (ранее ATRC был комитетом). При нём созданы рабочая группа для консультативных встреч АСЕАН+1 и суб-рабочая группа по управлению (радиочастотным) спектром для представительства на Всемирных радио-конференциях МСЭ [357]. На 13-м Совещании SOMTC (Вьентьян, 19–20.06.2013) было одобрено создание Рабочей группы по борьбе с киберпреступностью.

В 2015 г. вопросы обеспечения безопасности при использовании ИКТ выведены из компетенции Межсессионного совещания Регионального форума АСЕАН по борьбе с терроризмом и транснациональной преступностью (англ. «ARF ISM on CTTC») и переданы Межсессионному совещанию Регионального форума АСЕАН по безопасности ИКТ (англ. «ARF ISM on ICTs Security»).

Касательно Африканского союза отметим бóльший прогресс в развитии специализированных органов по кибербезопасности, нежели в IGAD. В 2019 г. была учреждена Экспертная группа по кибербезопасности. Политикой АС по расширению прав и безопасности детей в Интернете от 21.05.2024 предусмотрено

[357] Major Sectoral Bodies/Committees // ASEAN. URL: https://asean.org/our-communities/economic-community/asean-digital-sector/ (accessed 03.05.2025).

создание комитета по надзору за расширением прав и безопасности детей в Интернете. В рамках ШОС также нет совещаний и встреч руководителей и министров по тематике кибербезопасности.

Что касается представительных органов, то в Маскате расположен Инновационный центр Арабского региона по кибербезопасности при Международном союзе электросвязи (англ. «ITU-ARCC»), который управляется Национальным центром информационной безопасности Султаната и действует с 03.03.2013 на основании соответствующего соглашения[358]. При этом Региональный центр по борьбе с киберпреступлениями Управления по борьбе с наркотиками и преступностью ООН был открыт летом 2023 г. в Дохе (Катар). На уровне ШОС предлагается создание Центра ИИ для сокращения т.н. цифрового неравенства[359].

На **национальном** уровне, помимо органов общего характера, отметим специализированные органы, подразделения и организации, которые могут выполнять нормативную, координирующую, научно-исследовательскую, просветительскую, правоохранительную и связующую функции, одновременно совмещая, разделяя или делегируя их. Вне зависимости от подчинённости создаются министерства, управления, советы, центры по вопросам ИИ, цифровой экономики и удалённой работы, регулированию телекоммуникаций и цифрового правительства, цифровому благополучию, электронной безопасности, виртуальному пространству, Блокчейну, цифровой (электронной) сертификации, защите критической (информационной) инфраструктуры, а также CERT / CSIRT.

Примечательным является статус некоторых органов в сфере кибербезопасности, которые прошли путь от подразделений в сфере телекоммуникаций до отдельных ведомств. Например, созданное в 2006 г. Управление информационных технологий Султаната Оман в 2019 г. было преобразовано в Министерство транспорта, коммуникаций и информационных

---

[358] Oman ITU-Arab Regional Cybersecurity Centre // ITU. URL: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/Global-Partners/oman-itu-arab-regional-cybersecurity-centre.aspx (accessed 25.03.2025).

[359] SCO members invited to join new AI cooperation plan // Digwatch. 31.05.2025. URL: https://dig.watch/updates/sco-members-invited-to-join-new-ai-cooperation-plan (accessed 12.06.2025).

технологий Султаната Оман. Реорганизация имела место и в отношении Эфиопского агентства телекоммуникаций, созданного на основании Прокламации ФДРЭ № 49 от 1996 г., и Эфиопского агентства развития ИКТ, созданного на основании Прокламации ФДРЭ № 360 от 2003 г., чьи полномочия были переданы Министерству коммуникации и ИТ в 2011 г. (Прокламация ФДРЭ № 691 от 2010 г.)[360].

Наблюдается как укрупнение органов, так и расширение их компетенции. Например, полномочия Эфиопского телевещательного управления, учрежденного Прокламацией ФДРЭ № 178 от 1999 г., были переданы Эфиопскому управлению СМИ и расширены до регулирования и лицензирования онлайн СМИ, аналогового, кабельного, спутникового, цифрового ТВ и радио, Интернет-сервисов по подписке и без оплаты, агрегаторов контента, дистрибьютеров онлайн-контента, охватывая в том числе и деятельность в сети Интернет на основании Прокламации ФДРЭ № 1238 от 05.04.2021. Сходным образом 13.04.2021 были объединены Национальное управление криптографии и Департамент информационной безопасности Главного управления по применению информатики Министерства связи и информации РИ в Национальное управление по кибербезопасности и криптографии (решения президента Республики Индия №№ 53 и 133 от 2017 г., № 28 от 2021 г.).

Наибольший бюрократический аппарат среди стран Аравийской зоны наблюдается в Катаре (в частности, Вычислительный научно-исследовательский институт, экспертные комиссии по рискам, Национальный комитет по кибербезопасности, Центр расследования киберпреступлений[361], Национальное бюро по кибербезопасности – Национальные вопросы киберуправления и

---

[360] Yilma K.M., Abraha H.H. Указ. Соч.

[361] Сложность возникает из-за обозначения органов на английском и арабском языках. На самом деле сейчас это подразделение по экономическим и электронным преступлениям Главного управления уголовных расследований Министерства внутренних дел Государства Катар подобно Департаменту по борьбе с электронной преступностью в структуре полиции (Министерства внутренних дел) Государства Кувейт. См. подробней الإدارة العامة للمباحث الجنائية [Главное управление уголовных расследований] // Министерство внутренних дел Государства Катар. URL: https://portal.moi.gov.qa/wps/portal/MOIInternet/departmentcommittees/gacriminalinvestigation (дата обращения: 17.01.2025); إدارة مكافحة الجرائم الإلكترونية [Департамент по борьбе с электронной преступностью] // Министерство внутренних дел Государства Кувейт. URL: https://www.moi.gov.kw/main/sections/cyber-crime (дата обращения: 17.01.2025).

обеспечения, Комитет по регулированию искусственного интеллекта, Управление по регулированию связи, Цифровой инкубационный центр и Министерство связи и информационных технологий[362]) и в ОАЭ (Комитет по борьбе с киберугрозами и вредоносными программами, Управление по регулированию телекоммуникаций и цифрового правительства, Совет по цифровому благополучию, амбассадоры электронной безопасности, Центр электронной безопасности (Дубай), Цифровой центр Абу-Даби, Разведывательное управление сигналов [363] , Совет по кибербезопасности, Национальный совет по ИИ и Блокчейну при правительстве ОАЭ, Совет по цифровой экономике, Совет по искусственному интеллекту и передовым технологиям Абу-Даби и Центр цифровой сертификации)[364]. Тем не менее наблюдается тенденция централизации органов управления и регулирования в сфере кибербезопасности с чётко определённой компетенцией, в отличие от стран Глобального Севера, в том числе США[365].

Нормативными полномочиями по разработке от руководящих документов вплоть до законопроектов обладают как соответствующие министерства, так и отдельные специализированные органы по типу национальных управлений / агентств кибербезопасности, а в отдельных случаях и правоохранительные органы. Так, например, первоначально разработкой «антикиберпреступного» закона в ФДРЭ занималось Управление по безопасности информационных сетей (англ. «INSA»), а вторая и окончательная редакция была представлена генеральным прокурором.

CERT могут быть созданы на основании как законов, в том числе утверждённых в форме указов высших должностных лиц[366], так и подзаконных

---

[362] Заменил Высший совет по связям и информационным технологиям.

[363] Ранее Национальное управление по электронной безопасности.

[364] Seeger R. The New Battlefront: Cyber Security Across the GCC // Gulf International Forum. URL: https://gulfif.org/the-new-battlefront-cyber-security-across-the-gcc/ (accessed 12.01.2025).

[365] Shestak V.A., Tsyplakova A. D. Countering Cyberattacks on the Energy Sector in the Russian Federation and the USA // BRICS Law Journal. 2023. Vol. 10. No. 4. P. 35–52.

[366] Эта специфика касается в особенности королевств. Амрун (араб. «أمرن»), переводимый как указ, декрет и приказ, имеет множественные значения и в зависимости от государства может иметь разную силу. Вдобавок в некоторых странах по типу КСА неприменим термин «закон». См. подробнее Цыплакова А.Д. Некоторые юрислингвистические особенности источников

актов на уровне министров. Они получают жалобы о неуязвимости и запросы-предупреждения о киберинцидентах, разрабатывают рекомендации, политики, руководства, стандарты, проводят семинары по информационной безопасности для государственных органов, аудит и занимаются просвещением населения в сфере кибербезопасности, тем самым осуществляя превентивную функцию и оперативное реагирование. В отдельных случаях они оказывают помощь при расследовании киберпреступлений (в части цифровой криминалистики, например, JoCERT). В странах Аравийской зоны (и не только) они созданы как структурные единицы национальных центров по кибербезопасности, которые зачастую являются самостоятельными либо органами соответствующих министерств. В КСА, например, была изменена подчинённость CERT (от Комиссии по телекоммуникациям и информационным технологиям [367] к Национальному управлению по кибербезопасности).

В странах аль-Магриба компьютерные группы реагирования на чрезвычайные ситуации относятся к военным подразделениям. Например, maCERT входит в Генеральное управление безопасности информационных систем в составе Национальной администрации обороны.

Что касается азиатского региона, то CERT скорее самостоятельны или функционируют как структурные единицы министерств: в Индии CERT-In напрямую подчиняется Министерству электроники и информации, в КНР CERT/Координационный центр учрежден в 2001 г. как негосударственная организация. В Индонезии примечательно разделение сфер: ID-CERT действует как независимая организация и научный институт с 1998 г. [368] в тесном взаимодействии с узконаправленным государственным агентством — Индонезийской группой реагирования на инциденты безопасности в Интернете и

уголовного права и уголовного процесса арабских государств // Право между Востоком и Западом. 2025. № 1. С. 28-38.

[367] На данный момент именуется Комиссией по связи, космосу и технологиям с более широкими полномочиями.

[368] На официальном сайте ID-CERT указывается, что он учрежден в 1998 г. доктором Буди Рахарджо, однако данные разнятся, например, с Форумом команд по реагированию на инциденты и безопасности.

инфраструктуре/Координационным центром (англ. «ID-SIRTII/CC»), которая была создана позднее Министерским решением № 26/PER/M.KOMINFO/5/2007 от 04.05.2007 для надзора за безопасностью телекоммуникационных сетей на основе Интернет-протокола и подотчётна Министерству информации и телекоммуникаций Республики Индонезия. Академическая Группа реагирования на инциденты компьютерной безопасности (англ. «ID-ACAD-CSIRT») является некоммерческой негосударственной организацией по образованию и исследованию инициатив по безопасности[369].

Хронологически компьютерные группы реагирования на чрезвычайные ситуации учреждены в значительной мере в XXI в.: CERT-In — в 2004 г., Q-CERT — в 2005 г., SA-CERT — в 2006 г., aeCERT, EG-CERT — 2009 г., OCERT — в 2010 г., maCERT — в 2011 г., Bh-CERT, Kw-CERT, Ethio-CERT — в 2012 г., Tn-CERT — в 2020 г.

Активно обсуждается идея создания кибервойск для борьбы с терроризмом в Интернет-пространстве. По словам эксперта Абдулла Раззака Аль-Мурджана, террористические группы изменили свой подход и перешли к стратегии «скрытых единых сторонников» (араб. «المناصر المنفرد الخفي») в виртуальном пространстве. Ещё в сентябре 2015 г. она была реализована в отдельном государстве — в Кувейте была после нескольких серьёзных кибератак учреждена электронная армия[370]. После кибератаки на стратегическое агентство разведки Индонезийских национальных вооруженных сил в июне 2024 г. была выдвинута также идея о создании кибервойск в Республике, которая в доктрине обсуждалась ещё 10 годами ранее[371]. Конечно, в данном случае пока не идёт речи о проведении наступательных кибероперациях, как

---

[369] Setiadi F., Sucahyo Y.G., Hasibuan Z.A. An Overview of the Development Indonesia National Cyber Security. International Journal of Technology & Computer Science // 2012. №6. P. 106-114.

[370] إبراهيم العلبي. حرب سيبرانية.. هكذا تكافح دول الخليج الإرهاب إلكترونياً [Ибрагим Альби. «Кибервойна». Вот как страны Персидского залива борются с терроризмом в электронном виде.] // Alkhaleej. URL: https://alkhaleejonline.net/علوم-وتكنولوجيا/حرب-سيبرانية-هكذا-تكافح-دول-الخليج-الإرهاب-إلكترونياً (дата обращения: 25.03.2025).

[371] Isjchwansyah Y.R. Indonesia’s new cyber force needs to be planned, not rushed // ASPI. 17.09.2024. URL: https://www.aspistrategist.org.au/indonesias-new-cyber-force-needs-to-be-planned-not-rushed/ (accessed 25.03.2025), Ardiyanti H. Cybersecurity dan Tantangan Pengembangannya di Indonesia // Jurnal Politica. 2014. № 5 (1). P. 1–2.

в Государстве Япония с принятием закона о введении активной киберзащиты в мае 2025 г., хотя и является закономерным продолжением развития региональных инициатив. В 2021 г. ADMM предложил создать Центр передового опыта в области кибербезопасности и информации и Сеть киберзащиты для связи национальных центров операций по киберзащите, которые были открыты на морской военной базе Сингапура[372].

Хабы и отдельные проекты учреждаются для осуществления взаимодействия с частным сектором, расширяя государственно-частное партнёрство. В КСА, например, на сегодняшний день при поддержке Саудовской Федерации кибербезопасности, программирования и дронов (англ. «SAFCSP») действуют КиберХаб (араб. «سايبر هب», англ. «CyberHub»), к которому присоединились более 50 вузов (более 25 тысяч студентов) и на котором действует более 66 курсов, а также КодерХаб (араб. «كودر هب», англ. «CoderHub») (для программистов) и учебные лагеря Тувэйк[373] (араб. «طويق») по программированию, кибербезопасности, науке о данных, для молодёжи и 7/7[374].

Удобная для регистрации и финансирования стартапов площадка действует в Государстве Катар — цифровой инновационный центр (араб. «حاضنة الأعمال الرقمية»). Из 160 проектов уже 76 полноценно функционируют, было вложено 205,4 млн катарских риалов, 3,614 млн катарских риалов инвестиций в среднем приходится на один стартап[375].

---

[372] Harris G. The State of Cyber Defense Cooperation in ASEAN // Real Clear Defense. 31.01.2024. URL: https://www.realcleardefense.com/articles/2024/01/31/the_state_of_cyber_defense_cooperation_in_asean_1008628.html (accessed 25.03.2025).

[373] В августе 2019 г. была учреждена соответствующая академия. См. подробней: أكاديمية طويق [Тувэйк Академия]: официальный сайт. Эр-Рияд, Королевство Саудовская Аравия. URL: https://tuwaiq.edu.sa (дата обращения: 25.03.2025).

[374] سايبر هب [Киберхаб]: официальный сайт. Эр-Рияд, Королевство Саудовская Аравия. URL: https://cyberhub.sa (дата обращения: 25.03.2025); كودر هب [Кодерхаб]: официальный сайт. Эр-Рияд, Королевство Саудовская Аравия. URL: https://coderhub.sa (дата обращения: 25.03.2025); Our initiatives // Saudi Federation for cybersecurity, programming & drones. URL: https://safcsp.org.sa/en/portfolio#section-HakathonHomthem (accessed 25.03.2025).

[375] حاضنة الأعمال الرقمية [Цифровой инновационный центр]: официальный сайт. Доха, Катар. URL: https://dic.mcit.gov.qa/ar/ (дата обращения: 12.06.2025).

14.05.2025 закончились публичные обсуждения и консультации для финализации проекта Положения КСА «О Глобальном центре искусственного интеллекта» [376], который затрагивает создание и функционирование частных, расширенных и виртуальных хабов. Учреждение первых двух возможно на основании двустороннего соглашения. В последующем на основании решения Совета министров КСА будет назначен компетентный орган, который с его согласия утверждает создание виртуальных хабов провайдеров услуг и перечень иностранных государств, чьё право применимо к ним.

В части осуществления уголовного преследования реализованы три модели: создаются уполномоченные структурные подразделения в правоохранительных органах и судах, либо же традиционным органам предоставляются особые полномочия, либо отдельных должностным лицам делегируются полномочия по производству отдельных следственных (процессуальных) действий.

Что касается специализированных подразделений и органов, отметим иранскую полицию в сфере производства и обмена информацией (ФАТА), индийский апелляционный кибертрибунал, специализированные отделы по раскрытию и расследованию мошенничеств в сфере телекоммуникаций территориальных подразделений полиции КНР, отдел киберпатрулирования и Департамента по киберпреступлениям [377] Управления по расследованию преступлений Национальной полиции Республики Индия, а также судебно-медицинские (криминалистические) лаборатории по изучению цифровых следов при судебной полиции (e.g., в Королевстве Марокко).

Центр статистики и информационных технологий ИРИ совместно с Министерством связи и информационных технологий ИРИ ежегодно утверждает технические процедуры по хранению, защите, изъятию и предоставлению

---

[376] Global AI Hub Law // Istitlaa platform. URL: https://istitlaa.ncc.gov.sa/en/transportation/citc/globalailaw/Documents/Global%20AI%20Hub%20Law%20EN-AR%20-%20Final%20Draft%20for%20PC.pdf (accessed 18.05.2025).

[377] Ранее ИТ-департамент входил в Управление по расследованию специальных экономических преступлений. Kaburuan E.D., Damayanti A. The Effectiveness of Indonesian National Police Strategy in Cybercrime eradication through ASEAN Ministerial Meeting on Transnational Crime (AMMTC) // International Journal of Social Science and Human Research. 2022. № 5 (8). P. 3649-3661.

пользовательских данных и информации, а также практические рекомендации по поддержанию безопасности и надёжности данных и доводит их до сведения поставщиков услуг доступа и хостинга, а также пользователей[378].

Что касается сбора электронных доказательств, включая хранение, немедленное сохранение, проверку, изъятие и прослушивание телефонных разговоров, то отметим привлечение компетентных смежных органов. Например, если дело касается лиц и мест, связанных с судебной системой, а также организаций, связанных с центрами, с судебной системой, то указанные действия осуществляются Центром судебной защиты и информации ИРИ по распоряжению судебного органа (ст. 46 Постановления Главы судебной власти ИРИ от 03.08.2014 «Правила сбора и цитирования электронных доказательств», принятое во исполнение ст. 54 Закона ИРИ 2009 г.[379]). Комиссия же по коммуникациям и информационным технологиям КСА также оказывает помощь и техническую поддержку при расследовании преступлений в сфере информатики и во время судебного разбирательства (ст. 14 Положения КСА 2007 г.).

Второй версией проекта Прокламации ФДРЭ № 958/2016 предлагалась возможность представить полномочия по проведению цифровых расследований (англ. «digital forensic investigations») с физическим присутствием или дистанционно без судебного решения. Сходное положение было включено впоследствии в Прокламацию ФДРЭ № 808 от 02.01.2014 «О реорганизации Агентства по безопасности информационной сети»[380], однако для проведения расследований с физическим присутствием должностных лиц требуется судебное решение[381].

---

[378] Цыплакова А.Д. Борьба с киберпреступностью в странах Глобального Юга: сравнительно-правовое исследование / // Пролог: журнал о праве. 2025. № 1. С. 99–110.

[379] آیین نامه جمع آوری و استنادپذیری ادله الکترونیکی [Правила сбора и цитирования электронных доказательств] // Законодательная база ИРИ. URL: https://rc.majlis.ir/fa/law/show/897504 (дата обращения: 04.04.2025).

[380] Information Network Security Agency Reestablishment Proclamation No. 808/2013 // Federal Negarit Gazette. 2014. No. 6. P. 7129–7136.

[381] Yilma K.M. Указ. соч.

В части второй модели — особые полномочия судебной полиции (араб. «شرطة قضائية») по определению географического местонахождения подозреваемого или обвиняемого, средства совершения преступления, предметов преступления, а равно иных элементов, связанных с преступлением, с использованием ИКТ, информационной системы или технических механизмов, специально разработанных с данной целью согласно Закону АНДР № 04-18 от 25.12.2004 «О профилактике и предотвращении незаконного употребления и незаконного оборота наркотических средств и психотропных веществ» (с измен. и доп., введенными Законом АНДР № 05-23 от 07.05.2023)[382].

Относительно третьей модели отметим следующее. Согласно ст. 15 Закона Эмирата Рас-аль-Хэймату № 2 от 27.02.2023[383] сотрудники ответственного органа оазиса Рас-аль-Хэймату в сфере цифровых активов (англ. «RAK Digital Assets Oasis»), назначенные по решению Генерального прокурора по рекомендации Совета директоров, имеют полномочия (судебных) должностных лиц уголовного судопроизводства в доказывании деяний, совершенных в нарушение положений указанного закона и постановлений, принятых в соответствии с ним.

Подобно эмиратскому подходу нормами ст. 36 Закона Королевства Бахрейн № 30 от 12.07.2018 «О персональных данных» (далее — Закон КБ № 30-2018)[384] предусмотрена возможность назначения инспекторов (араб. «مفتشين») главой

---

[382] Закон АНДР № 04-18 от 25.12.2004 «О профилактике и предотвращении незаконного употребления и незаконного оборота наркотических средств и психотропных веществ» [قانون رقم ٠٤-١٨ مؤرخ في ١٣ ذي القعدة ١٤٢٥ الموافق ٢٥ ديسمبر سنة ٢٠٠٤، يتعلق بالوقاية من المخدرات والمؤثرات العقلية وقمع الاستعمال والاتجار غير المشروعين بها] // Официальный вестник Алжирской Республики. 2004. № 83. С. 3–8 и Закон АНДР № 05-23 от 07.05.2023 [القانون رقم ٢٣-٠٥ المؤرخ في ٧ مايو سنة ٢٠٢٣] // Официальный вестник Алжирской Республики. 2023. № 32. С. 13–17.

[383] Law No. 2 of 2023 on the establishment of RAK Digital Assets Oasis // RAK Legislative Committee. URL: https://www.rak.ae/wps/portal/rak/legislative-committee/legislation-search/!ut/p/z1/jZBBD4IwDIV_Eek2yNyO00TQZKJZRLeLWXTikgkkIr9fIF5Be2v7vb6XgoEzmMp2vrStrysb-l4bemFZSkmKiMzXcYwOuOAipzxVlMJpBBKMCeEJlgwxjsRW4aJYLXHGEjD_6NFECfRbb2aRDf0CcxFHYCaDchXoPuhi0kYmoIY7wZX-Fcbv7WrQBJE4IhEZVvY6TEHf3N2-Q9vY0kHzPJ6R3z-aTooP_T4FDQ!!/ (accessed 25.03.2025).

[384] قانون رقم ٣٠ لسنة ٢٠١٨ بإصدار قانون حماية البيانات الشخصية [Закон Королевства Бахрейн № 30 от 12.07.2018 «О персональных данных»] // Комиссия по законодательству и юридическим заключениям Королевства Бахрейн. URL: https://www.legalaffairs.gov.bh/HTM/K3018.htm (дата обращения: 25.03.2025).

Управления по защите персональных данных Королевства Бахрейн, которые имеют право входить в помещения с целью осмотра/наблюдения (араб. «معاينة») или *тафтишун*, получать доступ к файлам, записям, книгам, документам с существующими данными и к их копиям, а также заслушивать показания лиц.

Инспекторам, делегированным Министром юстиции, в силу решения, вынесенного по согласованию с соответствующим министром, предоставляется полномочия *мамурийя ад-добты аль-кодоийи*[385] (араб. «مأموري الضَّبْط القضائي») в отношении преступлений, подпадающих под их юрисдикцию и связанных с их должностями в рамках Закона КБ № 30-2018. Они также могут выполнять задачи, порученные им следственной комиссией (араб. «لجنة التحقيق»), которая формируется Управлением по защите персональных данных Королевства Бахрейн из делегированных инспекторов, сотрудников указанного управления и специалистов для расследования нарушений контролёром данных или уполномоченным лицом (дословно с араб. «مراقب حماية البيانات» — наблюдатель за защитой данными) по собственной инициативе, по получению запроса от Министра или на основе соответствующих отчётов и жалоб.

При выявлении признаков уголовно наказуемого деяния Совет директоров Управления по защите персональных данных Королевства Бахрейн направляет материалы в прокуратуру (ст. 55 Закона КБ № 30-2018).

Федеральным законом ОАЭ № 2 от 06.02.2019 «Об использовании информационно-телекоммуникационных технологий в сфере здравоохранения» [386] сотрудники министерств, агентств и департаментов в связи с исполнением указанного акта могут также наделяться статусом *мамурийя ад-добты аль-кодоийи*

---

[385] Подробнее о статусе см. Цыплакова А.Д. Должностные лица и органы, обеспечивающие реализацию полноты судебной власти, в арабских государствах: понятие и полномочия // Вестник Дальневосточного юридического института МВД России имени И.Ф. Шилова. 2025. № 2 (71). С. 142-151.

[386] قانون اتحادي رقم (2) لسنة 2019 في شأن استخدام تقنية المعلومات والاتصالات في المجالات الصحية [Федеральный закон Объединённых Арабских Эмиратов № 2 от 2019 года «Об использовании информационно-телекоммуникационных технологий в сфере здравоохранения»] // Официальная база законодательства ОАЭ. URL: https://uaelegislation.gov.ae/ar/legislations/1209 (дата обращения: 01.04.2025).

для расследования правонарушений, связанных с информационными системами Министерства здравоохранения ОАЭ.

Отдельного внимания заслуживают органы, действующие в СФЗ (ОЭЗ), а также в САР. Например, Управление по ценным бумагам и сырьевым товарам ОАЭ (далее — SCA) может предпринимать все действия, необходимые для периодического или внезапного контроля (араб. «إشراف»), надзора (араб. «رقابة») и обыска / осмотра (араб. «تفتيش») трёх категорий: лиц, предлагающих услуги в сфере виртуальных активов (оферентов; англ. «VASP»), лицензиатов и адресатов с целью обеспечения соблюдения решения № 23 от 01.11.2020, регулированию SCA и решениям, принятым во исполнение их, а также применимого законодательства. SCA может расследовать любые нарушения, выявленные в ходе проверки или включенные в любые жалобы, полученные SCA, а также запросить любые дополнительные разъяснения, информацию, документы или данные, которые оно сочтет это необходимым для целей контроля и расследования. SCA также может проверять компьютерные системы, компьютерные данные, трафику компьютерных данных или оборудование, где хранятся данные оферента, ответственной стороны в отношении предложения и лицензированного лица или получать доступ к ним.

Согласно Регулированию виртуальных активов и связанной с ними деятельности 2023 г.[387] в случаях, если Управление по регулированию виртуальных активов, регулирующее виртуальные активы в свободных зонах Дубая (англ. «VARA») обнаруживает поведение, которое, как оно подозревает, может быть связано с отмыванием денег, оно должно незамедлительно сообщать о своих подозрениях в соответствующий орган, осуществляющий полномочия и выполняющий функции в соответствии с соответствующим антиотмывочным законодательством — подразделение финансовой разведки Центрального банка ОАЭ, которое после изучения передаёт данные прокуратуре. Та, в свою очередь, может обращаться к VARA напрямую за получением более детальной информации.

---

[387] Virtual Assets and Related Activities Regulations 2023 // VARA. URL: https://rulebooks.vara.ae/node/18 (accessed 25.03.2025).

Все организации и их деятельность могут стать объектом расследования (англ. «investigation») и/или осмотра (англ. «examination») VARA в любое время любым способом, который VARA сочтет необходимым для целей осуществления своих полномочий, выполнения своих функций или достижения своих целей в соответствии с Законом Эмирата Дубай № 4 от 2022 г. «О регулировании виртуальных активов в Эмирате Дубай»[388].

Эмитенты виртуальных активов и VASP обязаны предоставить данные, объекты, книги, записи, счета, документы и другую информацию, запрошенные VARA как в бумажном, так и в электронном виде. Более того, фактически требования должны выполняться ещё в течение 10 лет после того, как деятельность субъекта перестаёт регулироваться VARA[389].

С учётом того, что опыт СЭЗ перенимается и африканскими, и азиатскими странами, идя даже дальше в части создания совместных хабов, может возникать уникальная ситуация с точки зрения подсудности, подследственности органов, а также применимого права. Так, например, 29.05.2025 Министерство связи, цифровых технологий и инноваций Ганны подписало меморандум о взаимопонимании с Корпорацией портов, таможни и свободной зоны Дубая и эмиратской компании «Presight AI» для создания Инновационного и технологического центра Ганы-ОАЭ[390].

В САР не только полицейские сотрудники, но и сотрудники таможенной и акцизной служб и т.н. инспекторы (должностное лицо, назначенный Министром торговли и экономического развития САР Гонконга) могут изымать контрафакт, непристойные материалы и собирать доказательства (ст. 36Б Закона САР Гонконга от 30.06.1997 «О контроле непристойных и неприличных материалов» (в ред. от

---

[388] Law No. (4) of 2022 Regulating Virtual Assets in the Emirate of Dubai // VARA. URL: https://rulebooks.vara.ae/sites/default/files/en_net_file_store/VARA_EN_338_VER1.pdf (accessed 25.03.2025).

[389] Волеводз А.Г., Цыплакова А.Д. О некоторых особенностях получения цифровых доказательств в арабских странах на примере Объединенных Арабских Эмиратов и Королевства Бахрейн // Российский следователь. 2025. № 1. С. 45-49.

[390] PCFC, Government of Ghana sign MoU to establish economic zone, digital incubator in Accra // WAM. 02.06.2025. URL: https://www.wam.ae/en/article/bjzgjpg-pcfc-government-ghana-sign-mou-establish-economic (accessed 02.06.2025).

23.05.2025)[391]. Управление по коммуникациям и уполномоченное в письменном виде должностное лицо могут арестовывать подозреваемых, обыскивать любые места, в отношении которых есть обоснованные предположения, что совершено правонарушение, а также где находятся или могут находиться доказательства (ст. 35 Закона САР Гонконг от 01.01.1963 «О телекоммуникациях» (в ред. от 01.10.2024)[392].

В качестве организационной особенности можно выделить инициативу Управления по регулированию телекоммуникаций и цифрового правительства ОАЭ — амбассадоры электронной безопасности — обучение студентов для продвижения деятельности aeCERT[393]. Подобная программа также реализуется в Омане, однако аудитория у неё более широкая: ИТ-специалисты (профессиональные амбассадоры), студенты (академические амбассадоры) и граждане либо резиденты Султаната (амбассадоры информационной безопасности)[394]. Схожая инициатива реализована в Республике Индия в рамках Индийского координационного центра киберпреступности (МВД) через киберволонтёров по трём направлениям: киберэксперты, промоутеры кибер-осведомлённости и киберволонтёры по удалению неправомерного контента[395]. В доктрине государств Глобального Юга отмечаются проблемы с образованием в сфере кибербезопасности[396]. По этой причине возрастает интерес к проектам по

---

[391] 淫亵及不雅物品管制条例 [Закон «О контроле непристойных и неприличных материалов»] // Законодательная база САР Гонконга. URL: https://www.elegislation.gov.hk/hk/cap390!en-sc?INDEX_CS=N (дата обращения: 06.06.2025).

[392] 电讯条例 [Закон О телекоммуникациях] // Законодательная база САР Гонконга. URL: https://www.elegislation.gov.hk/hk/cap106!en-sc?xpid=ID_1438402543810_002&INDEX_CS=N (дата обращения: 06.06.2025).

[393] السلامة السيبرانية والأمن الرقمي [Кибербезопасность и цифровая безопасность] // ОАЭ. URL: https://u.ae/ar-ae/information-and-services/justice-safety-and-the-law/cyber-safety-and-digital-security (дата обращения: 13.06.2025).

[394] أهداف برنامج سفراء السلامة المعلوماتية [Цели Программы послов информационной безопасности] // Национальный центр информационной безопасности Султаната Оман. URL: https://ambassadors.cert.gov.om/about_ar.aspx (дата обращения: 13.06.2025).

[395] Cyber Crime Volunteer Program // Vijetha IAS Academy. URL: https://vijethaiasacademy.com/blog/Cyber-Crime-Volunteer-Program (accessed 11.06.2025).

[396] Alqurashi R. K., AlZain M. A., Soh B., Masud M., Al-Amri J. Cyber Attacks and Impacts: A Case Study in Saudi Arabia // International Journal of Advanced Trends in Computer Science and Engineering. 2020. № 9 (1). P. 220.

объединению усилий представителей науки, правоприменительных органов и частного сектора. Одним из примеров подобного является Центр инноваций в области кибербезопасности Королевства Марокко, недавно учреждённый на основании совместного решения Министра высшего образования, научных исследований и инноваций и Министра экономики и финансов № 1148.25 от 06.05.2025 «Об утверждении соглашения о партнёрстве между Министерством цифрового перехода и административной реформы, Министерством высшего образования, научных исследований и инноваций, Управлением национальной обороны и Университетом Мухаммеда V в Рабата от 29.05.2024»[397].

§ 3. Инициативы по противодействию киберпреступлениям в отдельных странах Глобального Юга

Азия. Исходя из обозначенных институциональных механизмов, рассмотрим АСЕАН. ARF с 2004 г. проводит семинары и конференции по кибертерроризму, прокси-серверам, киберинцидентам, правовым и культурным мерам по укреплению; ATRC — с 2008 г. совместные воркшопы и учения с ЕС, Японией и КНР по вопросам безопасности сети; Встреча высших должностных лиц по социальному благосостоянию и развитию — с 2012 г. конференции по противодействию киберпроституции и киберпорнографии[398].

Арабский Восток. В 2012 г. Кувейт проводил Форум по управлению Интернетом в Арабском регионе, идея о котором возникла ещё на Всемирном форуме по управлению Интернетом в Рио-де-Жанейро в 2007 г. и была развита в октябре 2010 г. Экономической и социальной комиссией ООН для Азии и Тихого

---

[397] التوقيع على اتفاقية شراكة تهدف إلى إنشاء مركز للإبتكار في الأمن السيبراني [Подписание соглашения о партнерстве по созданию центра инноваций в области кибербезопасности] // Maacoom. 31.05.2024. URL: https://maacom.ma/2024/05/31/التوقيع-على-اتفاقية-شراكة-تهدف-إلى-إنش/ (дата обращения: 12.06.2025) و"المغرب يمهد لإقامة مركز سيبراني" [Марокко прокладывает путь к созданию «киберцентра»] // Hespress. 01.06.2025. URL: https://www.hespress.com/المغرب-يمهد-لإقامة-مركز-سيبراني-1569153.html (дата обращения: 12.06.2025)

[398] ASEAN's Cooperation on Cybersecurity and against Cybercrime. Presentation by the ASEAN Secretariat // Council of Europe. 04.12.2013. URL: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802f2393 (accessed 20.05.2025).

океана[399]. Одной из важных инициатив CERT являются киберучения. В 2020 г. проводились виртуальные учения по управлению киберрисками, связанными с удалённой работой, для арабских стран и других государств-членов Организации исламского сотрудничества[400]. С 2012 г. ITU-ARCC совместно с национальными CERT и OIC-CERT проводят подобные мероприятия ежегодно [401]. Зачастую принимающей стороной является O-CERT, в частности, по темам рисков криптовалют и возникающих угроз (18.09.2018), роста интеллекта вредоносных программ (17.09.2019), удалённой работы и киберугрозам (22.09.2020)[402].

Представители из 51 государства собирались несколько раз на хакатоны, проводимые SAFCSP: «Hajj Hackathon» в 2018 г., «Homathon» в 2020 г. (первый виртуальный в регионе)[403]. На региональном уровне симпозиум «Инновации в кибербезопасности и развитие индустрии» на Ближнем Востоке, организованный в Мускате 06.11.2022–09.11.2022 ITU-ARCC и Форумом команд реагирования на чрезвычайные ситуации и совмещённый с 10-ой встречей и 14-ой ежегодной конференцией OIC-CERT и 10-ым региональным саммитом по кибербезопасности [404]. Месяцем позднее (06.12.2022–08.12.2022) Арабский международный саммит «Содействие глобальному сотрудничеству в области кибербезопасности» проводился под руководством Национального центра по кибербезопасности Королевства Бахрейн, охватывая вопросы туристического,

---

[399] AlShatti Q. The launch of the Arab IGF // DiploFoundation. 28.10.2013. URL: https://www.diplomacy.edu/blog/launch-arab-igf/ (дата обращения: 12.06.2025).

[400] الهيئة الوطنية للأمن السيبراني تشارك في تمرين افتراضي بحضور 25 دولة عربية وإقليمية [Национальное управление по кибербезопасности участвует в виртуальных учениях в присутствии 25 арабских и региональных стран] // Национальный центр безопасности KCA. URL: https://cert.gov.sa/ar/media-center/news/cyber-drill-2020/ (дата обращения: 25.03.2025).

[401] The 10th Regional cybersecurity Arabic regional and OIC-CERT drill kicks off // Ministry of Transport, Communications and Information Technology of Sultanate of Oman. 06.11.2022. URL: https://mtcit.gov.om/ITAPortal/MediaCenter/NewsDetail.aspx?NID=81251 (accessed 25.03.2025).

[402] Cyber Drill // OIC CERT. URL: https://www.oic-cert.org/en/events/cyber_drill/index.html (дата обращения: 25.03.2025).

[403] Our initiatives // Saudi Federation for cybersecurity, programming & drones. URL: https://safcsp.org.sa/en/portfolio#section-HakathonHomthem (дата обращения: 25.03.2025).

[404] Annual conference: 2022 // OIC-CERT. URL: https://www.oic-cert.org/en/events/conference/2022.html (дата обращения: 25.03.2025).

строительного, финансового, медицинского секторов, а также правоохранительной деятельности[405].

На межгосударственном уровне Генеральный секретариат ССАГПЗ в сотрудничестве с Арабским бюро образования организует периодические семинары по стратегии информационной безопасности образования. Так, в ходе встречи летом 2023 года специалистов в области информационной безопасности в странах ССАГПЗ в Маскате Министерство образования Султаната Оман приняло рабочий документ с дорожной картой электронного образования, проектом умных школ и использованием ИИ в школьном образовании[406].

На **Африканском** континенте (да и на Ближнем Востоке) значительная часть мероприятий проводится при поддержке региональных и универсальных организаций, а также стран Глобального Севера. Так, например, в рамках СЕ и ЕС запущено два проекта: КиберЮг (июнь 2017 г. – декабрь 2023 г.) и КиберЮг+ (01.01.2024 – 31.12.2026). Их участники — АНДР, ИХК, Ливан, Марокко, Тунис, Палестина, Ливия, АРЕ, Сирия, Израиль[407]. Советом Европы 01.08.2023 также был запущен проект «Усиленные глобальные действия по противодействию киберпреступности» (англ. «GLACY-e») до 31.01.2026 в поддержку стран Латинской Америки, Африки и АТР[408]. Проводятся конференции, встречи, воркшопы, семинары по электронным доказательствам, онлайн защите несовершеннолетних, криптовалютам, международному сотрудничеству,

---

[405] القمة العربية الدولية للأمن السيبراني [Арабский саммит по кибербезопасности] // Управление информации и электронного правительства Королевства Бахрейн. URL: https://www.iga.gov.bh/article/arab-international-cybersecurity-summit (дата обращения: 25.03.2025).

[406] استقبلت وزارة التربية والتعليم وفد يضم عددًا من المختصين بمجال أمن المعلومات في دول مجلس التعاون الخليجي، بحضور سعادة الأستاذ الدكتور عبدالله بن خميس أمبوسعيدي وكيل الوزارة للتعليم، وذلك بقاعة نزوى بديوان عام الوزارة، وتأتي هذه الزيارة في إطار إبراز جهود أمن المعلومات التعليمية في الوزارة. [Министерство образования приняло делегацию, включающую ряд специалистов в области информационной безопасности в странах Совета сотрудничества залива, в присутствии заместителя министра образования Абдуллы бин Хамиса Амбусаиди в зале Низва главного офиса министерства, и этот визит проходит в рамках освещения усилий министерства по обеспечению информационной безопасности в сфере образования] // Educational Portal. 25.08.2023. URL: https://home.moe.gov.om/region/alwesta/topics/1/show/9843 (дата обращения: 25.03.2025).

[407] Последние две страны приглашались для участия только в первом проекте.

[408] GLACY-e // Council of Europe. URL: https://rm.coe.int/3399-glacy-e-summary-vfinal-en/1680ae1cba (accessed 06.06.2025).

экспертизе данных в реальном времени, ИИ, имплементации Будапештской конвенции и дополнительных протоколов к ней, сети 24/7, онлайн сексуальному насилию, учения по расследованию, а также комплексные оценки действующего законодательства, разрабатываются рекомендации по совершенствованию правовых основ и институциональных механизмов[409].

Первый форум по киберпреступности АС состоялся при поддержке УНП ООН, СЕ, ЕС, Интерпола, Содружества Наций, Великобритании и США 16–18.10.2018, второй — при поддержке СЕ 28–29.06.2021 [410] . 20–30.05.2024 АФРИПОЛ при поддержке Интерпола провёл обучение по использованию инструментария для расследования киберпреступлений, ОСИНТ, виртуальных активов[411].

На **национальном** уровне также проводятся соответствующие учения общего характера и по секторам. Так, например, с 2013 г. Q-CERT проводит ежегодные учения «Звезда» (араб. «نجم»); в 2022 г. приняли участие 125 государственных и негосударственных учреждений (1 400 участников, что на 20 % выше, чем в предшествующем году) [412] . Совет по кибербезопасности ОАЭ 21.03.2022 провёл виртуальные учения «Кибер 193» совместно с представителями 140 стран, Экспо 2020 Дубай и Международным союзом электросвязи с помощью видеоконференцсвязи и методов облачных вычислений реализовали более 20 сценариев симулирования электронных атак[413].

---

[409] CyberSouth // Council of Europe. URL: https://rm.coe.int/3692-cybersouth-v13-extension-dec2021/1680a4d2a0 (accessed 06.06.2025); CyberSouth+ // Council of Europe. URL: https://rm.coe.int/3529-cybersouth-outline-en-v10-05-04-2024/1680af3217 (accessed 06.06.2025).

[410] The First African Forum on Cybercrime // African Union. URL: https://au.int/en/newsevents/20181016/first-african-forum-cybercrime (accessed 06.06.2025); Press releases. The African Union Convenes The Second African Cybercrime Forum // African Union. 08.06.2021. URL: https://au.int/fr/node/40556 (accessed 06.06.2025).

[411] African Union strengthens investigation capabilities on virtual assets and cybercrime // African Union. 22.05.2024. URL: https://au.int/ar/node/43809 (accessed 06.06.2025).

[412] National Cyber Security Agency Honors 125 Entities for Participating in 2022 STAR Drill // Qatar News Agency. 29.06.2022. URL: https://www.qna.org.qa/en/News-Area/News/2022-06/29/0052-national-cyber-security-agency-honors-125-entities-for-participating-in-2022-star-drill (accessed 25.03.2025).

[413] Spence N. UAE Cybersecurity Council holds virtual exercise ‘Cyber 193’ with 140 countries // Security Middle East Magazine. 21.03.2022. URL: https://www.securitymiddleeastmag.com/uae-cybersecurity-council-holds-virtual-exercise-cyber-193-with-140-countries/ (accessed 25.03.2025).

Осенью того же года Национальное управление по кибербезопасности КСА совместно с саудовской информационно-технологической компанией «Сайт» (араб. «سايت», англ. «SITE») запустило национальную программу киберучений в рамках механизма «КиберК» (араб. «سايبرك», англ. «CyberIC»). Она предоставляет современные симуляции, чтобы помочь получить знания и научить слушателей лучшим мировым практикам защиты от кибератак. Управление КСА следит за упражнениями и предоставляет организациям обратную связь о том, как они могут улучшить свои возможности и операции[414].

В 2017 г. Управление по информации и электронному правительству Королевства Бахрейн вместе с Лабораторией Касперского провело первые учения электронных ястребов — интерактивная симуляция защиты для специалистов из государственных учреждений[415]. В рамках национальной программы упражнений по электронной безопасности Национальный центр по кибербезопасности Королевства Бахрейн производит моделирование виртуальных потенциальных кибератак, а также оценку рисков, угроз, и предлагает способы противодействия, улучшения мониторинга и нейтрализации последствий как для отдельных учреждений, так и для целых секторов. Подобный проект уже был реализован в феврале 2022 г. для финансовой сферы, а для других запланирован на 3-й/4-й кварталы 2023 г. (например, ТЭК — октябрь 2023 г.)[416].

CERT реализуют пропагандистские и просветительские кампании посредством создание широкой библиотеки информационных плакатов, обучающих видео как на арабском языке, так и на языке жестов в области советов

---

414 The National Cybersecurity Authority launches the “National Program for Cyber Drills” // National Cybersecurity Authority of the Kingdom of Saudi Arabia. 14.11.2022. URL: https://nca.gov.sa/en/news?item=372 (accessed 25.03.2025).

415 Information & eGovernment Authority Organizes First Cyber Drill for Cyber Hawks in Partnership with Kaspersky Lab // Kaspersky Lab. 11.10.2017. URL: https://me-en.kaspersky.com/about/press-releases/2017_information-egovernment-authority-organizes-first-cyber-drill (accessed 25.03.2025).

416 اختبار الجاهزية الوطنية [Национальный текст готовности] // Национальный центр по кибербезопасности Королевства Бахрейн. URL: https://www.ncsc.gov.bh/ar/programs-initiatives/national-cyber-capabilities/national-cyber-drill.html (дата обращения: 25.03.2025); مبادرة التمارين السيبرانية للقطاعات الحيوية [Национальная инициатива по киберучениям в секторах] // Национальный центр по кибербезопасности Королевства Бахрейн. URL: https://www.ncsc.gov.bh/ar/programs-initiatives/national-cyber-capabilities/sectoral-cyber-drill.html (дата обращения: 25.03.2025).

по созданию паролей, разъяснений киберрисков и руководства по электронной коммерции, основного понятийного аппарата, шагов, необходимых для снижения виктимости от ряда преступлений в киберпространстве, рекомендаций по дистанционному обучению и онлайн-встречам, использованию программного обеспечения VPN и по многим другим темам, которые предназначены не только для профессиональных пользователей (IT-специалистов), но и остальных пользователей ПК и сети «Интернет», а также разрабатывают единообразные формы измерения зрелости кибербезопасности для оценки по трём показателям: процессы, практики и люди (см. Приложение № 7 в качестве образца) [417]. К учебным проектам для профилактики киберпреступлений и подготовки квалифицированных кадров следует отнести двуязычные платформы «Haseen» Министерства транспорта и коммуникаций и Министерства среднего и высшего образования в Катаре и «SafeSurf» Министерства коммуникаций и информационных технологий в Катаре, бесплатную образовательную платформу «Линия» или «Сатр» (араб. «سطر», англ. «SATR») SAFCSP, предоставляющую бесплатный интегрированный контент по программированию: учебники, курсы, 2 572 видеоклипа, 67 проектов, 390 тестовых вопросов, 333 статьи [418]. Центры по кибербезопасности также проводят мероприятия по повышению киберосведомлённости. Например, I4C проводит т.н. «Cyber Jaagrookta Diwas» каждую первую среду ежемесячно в школах, колледжах и университетах, разъясняя базовые правила кибергигиены[419].

Что касается действующих систем по противодействию киберпреступлений (пресекательных инициатив), отметим национальные и региональные проекты по выявлению уязвимостей, подозрительных IP-адресов, межведомственному обмену информацией, онлайн-регистрации сообщений о преступлениях (порталы МВД

---

[417] التوعية الأمنية [Повысить осведомлённость] // Национальный центр безопасности КСА. URL: https://cert.gov.sa/ar/awareness/?page=1 (дата обращения: 25.03.2025) и Шестак В.А., Цыплакова А.Д. Виктимологическая профилактика киберпреступлений в Королевстве Саудовская Аравия // Мировой судья. 2024. № 4. С. 2–7.

[418] سطر [Линия]: официальный сайт. Эр-Рияд, Королевство Саудовская Аравия. URL: https://satr.codes (дата обращения: 25.03.2025).

[419] CYBER JAAGROOKTA // I4C. URL: https://i4c.mha.gov.in/cyber-jagrookta.aspx (accessed 25.03.2025).

или прокуратур по всем или отдельным видам) и выявлению «обеляемых» преступных активов. Так, например, в июле 2020 года GCC-CERT был представлен совместный проект на шестом собрании министерского комитета по электронному правительству — платформа по анализу и пресечению вредоносного программного обеспечения[420]. На национальном уровне в КСА под эгидой SAFCSP была создана первая ближневосточная платформа вознаграждений за выявление уязвимостей (араб. «منصة مكافآت الثغرات», англ. «Bug Bounty»). Более 300 компаний и 15 тысяч специалистов уже подключены к ней[421].

Исполнительный комитет электронного правительства ССАГПЗ запустил систему подозрительных Интернет-адресов (араб. «نظام عناوين الانترنت المشبوهة», англ. «IP Reputation»), которая позволяет центрам реагирования на компьютерные чрезвычайные ситуации отслеживать подозрительные Интернет-адреса по всему миру, чтобы предотвратить киберугрозы[422].

На основании Положения КСА от 21.04.2014 «О передаче информации о клиентах с частными средствами в Национальный информационный центр при Министерстве внутренних дел (Система безопасности Шумуусун)»[423] внедрена соответствующая система. Информация передаётся через сети, лицензированные Комиссией по связи, космосу и технологиям КСА с целью контроля за правонарушителями и развития сотрудничества в сфере туризма: отели, апартаменты, прокат транспортных средств и офисов, ювелирные магазины, интернет-кафе, компании по недвижимости, частные жилые комплексы, частные

---

[420] GCC Malware Analysis Platform Launched // Bahrain News Agency. 20.07.2020. URL: https://www.bna.bh/en/GCCMalwareAnalysisPlatformlaunched.aspx?cms=q8FmFJgiscL2fwIzON1%2BDtn0tM2%2FwwMJUBiBhb5CV%2Fc%3D (accessed 25.03.2025).

[421] Bug Bounty: official website. URL: https://bugbounty.sa (accessed 25.03.2025).

[422] اللجنة الوزارية للحكومة الالكترونية بدول مجلس التعاون تعقد اجتماعها الخامس في البحرين [Комитет министров электронного правительства стран Персидского залива проводит свое пятое заседание в Бахрейне] // Исполнительный комитет электронного правительства ССАГПЗ. 21.03.2017. URL: http://www.gcc-egov.org/ar/news_details?id=758559 (дата обращения: 25.03.2025).

[423] (نظام نقل معلومات المتعاملين مع المنشآت الخاصة إلكترونياً إلى مركز المعلومات الوطني في وزارة الداخلية (نظام شموس الأمني [Положение КСА от 21.04.2014 «О передаче информации о клиентах с частными средствами в Национальный информационный центр при Министерстве внутренних дел (Система безопасности Шумуусун)»] // Бюро экспертов Совета министров КСА. URL: https://laws.boe.gov.sa/BoeLaws/Laws/LawDetails/ad0354f7-9756-4a4e-8948-a9a700f19705/1 (дата обращения: 25.03.2025).

охранные компании, общественный транспорт. Общественная парковка, магазины подержанной мебели, автомобильные магазины, оздоровительные и развлекательные учреждения[424]. С одной стороны, Шумуусун позволил в 2013 г. выявить более 70 тысяч разыскиваемых лиц[425]. С другой — значительно снижены затраты организаций на установку, эксплуатацию и обслуживание компьютерных систем, настроена архитектура для автоматизации обмена информацией, поскольку подключение к сервису бесплатное[426].

В Республике Индия 30.08.2019[427] МВД запустило Национальный портал отчётности о киберпреступности[428], с которого сообщения автоматически направляются в компетентные правоохранительные органы штатов или союзных территорий для дальнейшего анализа и принятия решения в соответствии с положениями закона. Вдобавок на указанном портале хранится репозитарий подозреваемых (абонентские номера, электронные почтовые ящики, Интернет-ресурсы, ID мессенджеров), размещены чат-бот «Вани» и модуль «Система отчетности и управления гражданским финансовым кибермошенничеством» (англ. «Citizen Financial Cyber Fraud Reporting and Management System»). Резервный Банк Индии запустил также на основании ИИ ПО «Охотник на мулов» (англ. «MuleHunter») для отслеживания т.н. денежных мулов[429], используемых в

---

[424] شموس [Шумуусун] // Министерство внутренних дел КСА. URL: https://www.moi.gov.sa/wps/portal/Home/sectors/publicsecurity/publicsecurity/shomoos/ (дата обращения: 19.06.2025).

[425] «نظام شموس عبر ومخالف مطلوب ألف 70 لـ الوصول تؤكد «الداخلية» [Министерство внутренних дел подтверждает прибытие 70 тысяч разыскиваемых и нарушителей через систему Шумуусун] // Новости «عكاظ». 14.05.2013. URL: https://www.okaz.com.sa/article/570285/-70-ل-الوصول-تؤكد-الداخلية-شموس-نظام-عبر-ومخالف-مطلوب-ألف (дата обращения: 19.06.2025).

[426] Tsyplakova A.D. Comprehensive approach to cybercrime prevention in Arab countries // Law, State and Telecommunications Review. 2025. № 17-1. P. 23–41, Цыплакова А.Д. Борьба с киберпреступностью в странах Глобального Юга: сравнительно-правовое исследование // Пролог: журнал о праве. 2025. № 1. С. 99–110.

[427] 20.01.2020 представлен общественности.

[428] National Cyber Crime Reporting Portal: official website. URL: https://cybercrime.gov.in (accessed 11.06.2025).

[429] Некоторую аналогию можно провести с феноменом дроппера в РФ. Tsyplakova A. Foreign Approaches to Droppers. III All-Russian Academic Hearings of Laws and Bills in the field of digital security. MGIMO University, Irkutsk, 9 July of 2025. URL: https://ssrn.com/abstract=5348975 (accessed 14.07.2025).

мошеннических схемах и ОД/ФТ[430]. Это напоминает усовершенствованный портал для хавалдар «goAML»[431] в арабских (и не только) странах и эмиратский проект «Фаури Тик» (араб. «فوري تيك»)[432].

С учётом транснационального характера киберпреступности важно не только укрепление национальной инфраструктуры и создание соответствующих технических мощностей и кадровых ресурсов, но и сокращение т.н. цифрового разрыва, поэтому важно объединение усилий на межгосударственном уровне.

Подводя итог криминологической части исследования, можно выделить несколько направлений развития руководящих документов. Во-первых, по уровню: региональный и национальный — предполагает скорее параллельное развитие. Азиатский регион по хронологии (2010-е гг.) значительно опережает африканский и арабский (2020-е гг.), хотя в меньшей мере затрагивает напрямую именно уголовно-правовую область и уже по объёму. На национальном уровне отметим обновление стратегий примерно раз в 5–7 лет и схожую структуру: цели и корреспондирующие задачи, необходимые для реализации проекты и инициативы. Сферами деятельности являются не только физическая и кибербезопасность (реагирование на инциденты, выявление уязвимостей), но и технологические мощности и человеческие ресурсы, порядок взаимодействия в части вертикального и горизонтального сотрудничества (государственно-частное партнёрство, международное сотрудничество), образование (подготовка кадров и совершенствование процессов), культура (воспитание и кибергигиена) и экономические процессы (цепочки поставок, платежи). Зачастую руководящие

---

[430] Various measures have been taken by the government to strengthen cyber security in the financial sector // PIB Dehli. 18.03.2025. URL: https://www.pib.gov.in/PressReleasePage.aspx?PRID=2112323 (дата обращения: 11.06.2025).

[431] Программное обеспечение разработано Службой информационных технологий УНП ООН в партнерстве с Глобальной программой УНП ООН по борьбе с отмыванием денег, преступными поступлениями и финансированием терроризма (англ. «GPML») для ПФР. См. подробнее Проект ООН // УНП ООН. URL: https://www.unodc.org/unodc/en/global-it-products/goaml.html (дата обращения: 16.05.2025).

[432] О правовом статусе хавалдар и системах см. Шестак В.А., Цыплакова А.Д. Противодействие отмыванию денежных средств, полученных преступным путем: опыт Объединенных Арабских Эмиратов // Вестник Университета прокуратуры Российской Федерации. 2023. № 4 (96). С. 117–122.

документы разрабатываются скорее уполномоченными органами, нежели высшими должностными лицами (Индонезия и СО как исключения), что можно объяснить более простой процедурой принятия, внесения изменений и обновления, а также оперативным учётом специфики проблем в рассматриваемой сфере, хотя выявлены и отдельные пробелы в части, например, квантовых технологий. Они отражают сложившиеся тенденции развития государств.

Во-вторых, с точки зрения предмета регулирования выделяются как общие, так и секторальные документы, охватывающие, но не ограничивающиеся электронными коммуникациями, транзакциями и подписями, защитой и конфиденциальностью персональных данных, интеллектуальной собственности, стандартов контента, электронных платежных систем, защитой потребителей или бенефициаров, управление Интернетом и ИТ, цифровым правительством и автоматизацией процессов, электронным документооборотом, использованием искусственного интеллекта.

В-третьих, в качестве отдельного направления можно выделить криминалистически значимые руководства (белые книги), разрабатываемые как представителями науки, так и правоприменителями, а также стандарты и руководства органами, ответственными за кибербезопасность в стране.

С точки зрения изученных институциональных механизмов констатируем на региональном уровне различные министерские встречи, рабочие группы, исполнительные комитеты и CERT; на национальном уровне — общую тенденцию к наделению целых ведомств или корреспондирующих структурных подразделений широкими полномочиями по координации деятельности, разработке нормативного и технического регулирования, научно-исследовательских и просветительских проектов, а также вспомогательными функциями при расследовании инцидентов и преступлений. Развитый бюрократический аппарат прошёл в большинстве рассмотренных стран Глобального Юга долгий путь становления от подотчётного структурного подразделения до самостоятельного компетентного органа с расширением компетенций. Фактически любой орган, имеющий ЭДО, АСОД,

действует в виртуальном пространстве и прямо или косвенно формирует как базу противодействия, так и сталкивается с рисками и угрозами.

Уникальной представляется ситуация с точки зрения ОЭЗ (СФЗ) и САР, где отдельные должностные лица или органы могут собирать информацию, которая может лечь в основу для возбуждения уголовных дел, производить (в т.ч. по поручению и без такового) процессуальные действия, что способствует всестороннему эффективному пресечению посягательств. Также выявлена тенденция привлечения в качестве лиц, обладающих специальными знаниями и/или полномочиями для осуществления следственных действий, должностных лиц органов исполнительной власти.

Особое место отводится профилактической деятельности, которой «пронизаны» все уязвимые сектора и социальные группы, которая выходит за пределы одного государства (а порой и региона) и охватывает прежде всего просвещение: учреждение амбассадоров среди студентов, граждан, профессионалов и в академической среде, создание учебных лагерей, образовательных ресурсов и проектов, платформ для сообщений о киберпреступлениях, проведение кампаний, форумов, интенсивов, семинаров, развитие стартапов и инновационных центров, — стандартизацию, сертификацию, регулярное проведение оценок уровня кибербезопасности, проведение киберучений общего характера и по секторам на нескольких уровнях, в т.ч. хакатоны (просветительные и технико-экономические инициативы), а также аккумулирование баз данных как на национальном, так и на региональном уровнях, в частности систему ССАГПЗ подозрительных Интернет-адресов (араб. « نظام عناوين الانترنت المشبوهة», англ. «IP Reputation»), централизованную автоматизированную систему безопасности КСА «Солнца» (араб. «شموس»; Шумуусун), ближневосточную платформу по выявлению уязвимостей (араб. «منصة مكافآت الثغرات», англ. «Bug Bounty»), индийские и эмиратские системы в сфере ПОД/ФТ по типу «MuleHunter», «goAML», «Фаури Тик», а также комплексные порталы для оперативного сообщения о преступлениях — пресекальные инициативы.

Отдельные перечисленные инициативы стран Глобального Юга могут быть восприняты как образцовый зарубежный опыт не только для конкретной национальной правовой системы, но и для межведомственного или межгосударственного уровней. Например, киберволонтёры, электронные амбассадоры, комплексные базы данных по проверке подозреваемых контактных данных, Интернет-ресурсов, IP-адресов, отдельных категорий УНФПП, как доступных общественности, так и закрытых (для правоохранительных целей).

Таким образом, противодействие киберпреступлениям — это комплексная деятельность правоохранительных и специализированных государственных органов, органов законодательной и судебной властей, должностных лиц, физических и юридических лиц (и подобных им корпоративных образований) на горизонтальном и вертикальном, внутри- и межгосударственном уровнях, включающая разработку нормативных правовых актов, стандартов, руководств и стратегий, профилактические (просветительские), экономико-технические и пресекательные инициативы, борьбу с киберпосягательствами (выявление, раскрытие, расследование кибердеяний, уголовное преследование за них, в том числе наложение ограничительных, обеспечительных и иных процессуальных мер) и осуществление в связи с этим международного сотрудничества в двустороннем и многостороннем форматах[433].

[433] Цыплакова А.Д. Противодействие киберпреступлениям в странах Глобального Юга: современное состояние, проблемы и перспективы / А.Д. Цыплакова // Право и управление. XXI век. — 2025. — № 3. — С. 62–75.

ГЛАВА III. УГОЛОВНО-ПРОЦЕССУАЛЬНЫЕ МЕРЫ ПРОТИВОДЕЙСТВИЯ КИБЕРПРЕСТУПЛЕНИЯМ В ОТДЕЛЬНЫХ СТРАНАХ ГЛОБАЛЬНОГО ЮГА

§ 1. Особенности расследования киберпреступлений и доказывание в отдельных странах Глобального Юга

При расследовании как киберпреступлений, так и традиционных деяний особую значимость имеют электронные (цифровые) доказательства и следы. В нормативно-правовой базе стран Глобального Юга нет единого терминологического подхода, причём даже в рамках одного и того же государства. Например, в Положении КСА от 17.04.2020 «О коммерческих судах»[434] указано *электронное* доказательство (араб. «الإثبات الإلكتروني» / «الدليل الإلكتروني»), в то время как в Положении КСА от 07.01.2022 «О доказательствах» (далее — Положение КСА 2022 г.)[435] — *цифровое* доказательство.

В юридической литературе до сих пор ведутся дебаты относительно правильности понятия (электронный или цифровой). По мнению некоторых учёных-юристов, электронный и цифровой соотносятся как общее и частное[436], что подтверждается и нормативным подходом: согласно ст. 1 ФДЗ ОАЭ № 34-2021 *электронный* означает связанный с электромагнитной, фотоэлектрической, цифровой, автоматизированной, фотоэлектрической или аналогичной технологией.

В настоящем исследовании понятия будут использоваться в качестве взаимозаменяемых с акцентом на то, какое применимо в отношении конкретного государства или языка (см. Приложение № 8).

---

[434] نظام المحاكم التجارية [Положение «О коммерческих судах»] // Бюро экспертов Совета министров КСА. URL: https://laws.boe.gov.sa/BoeLaws/Laws/LawDetails/38334008-3b70-4c6c-b3af-aba3016a8061/1 (дата обращения: 09.03.2025).

[435] نظام الإثبات [Положение Королевства Саудовская Аравия от 07.01.2022 «О доказательствах»] // Бюро экспертов Совета министров КСА. URL: https://laws.boe.gov.sa/BoeLaws/Laws/LawDetails/2716057c-c097-4bad-8e1e-ae1400c678d5/1 (дата обращения: 09.03.2025).

[436] مبارك بن محمد الخالدي. الإثبات بالدليل الرقمي وتطبيقاته القضائية: دراسة فقهية مقارنة بنظام الإثبات السعودي // مجلة قضاء. ٢٠٢٤. ٣٢٩-٤١٦. [Мубарак бин Мухаммад Аль-Халиди. Доказательство с помощью цифровых доказательств и его судебное применение: юриспруденческое исследование в сравнении с саудовской системой доказательств // Судебный журнал. 2024. С. 329-416 (на араб. яз.).]

В качестве правовой основы выступают киберзаконы, уголовно-процессуальное, а также гражданско-процессуальное регулирование, применимое в качестве *lex specialis*, что характерно как для ряда арабских государств, так и для ИРИ и Республики Индонезия[437]. В качестве примера можно привести Закон Республики Индонезия № 11 2008 г. «Об электронной информации и трансакциях»[438], решение Министра юстиции КСА № 921 от 12.10.2022 «Контроль процедур электронного доказательства»[439].

При определении правового статуса электронных доказательств отметим как их полную самостоятельность (ФДРЭ, ИХК, Катар), так и встраивание в традиционные доказательственные начала: вещественные доказательства, полученные в ходе судебной экспертизы (ОАЭ, АРЕ, ранее КНР[440]), носитель информации, который может быть приравнен либо к письменной форме документов (ОАЭ, КСА, Индия), — а равно признание электронной формы доказательств (Индия). В отдельных случаях не прослеживаются и общие начала для признания цифровых доказательств как отдельного вида доказательств (АНДР, КМ).

---

[437] هادی تبار, اسماعیل, یعقوبی گلوردی, محمد کاظم. ادله اثبات الکترونیکی در دادرسی‌های کیفری در نظام حقوقی ایران // فقه جزای تطبیقی. ۲۰۲۳. ۳ (۱). ۱۲۳-۱۱۳. [Хади Табар, Исмаил, Якуби Глорди, Мохаммад Казем. Доказательства электронных доказательств в уголовном процессе в правовой системе Ирана // Сравнительное уголовное правоведение. 2023. № 3 (1). С. 113-123 (на перс. яз.)]; خسروی زاد, افشار, سپهری, روح الله, بابایی, حمیده. مشروعیت تحصیل دلیل در جرایم فضای مجازی در حقوق جزایی ایران // فقه جزای تطبیقی. ۲۰۲۲. ۲ (۳). ۸۵-۷۵ [Хосравизад, Афшар, Сепери, Рухолла, Бабаи, Хамида. Легитимность изучения доказательств преступлений в киберпространстве в уголовном праве Ирана // Сравнительное уголовное правоведение. 2022. № 2 (3). С. 75-85].

[438] Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik [Закон Республики Индонезия № 11 2008 г. «Об электронной информации и трансакциях»] // База законодательства Республики Индонезия. URL: https://peraturan.bpk.go.id/Details/37582/uu-no-19-tahun-2016 (дата обращения: 19.03.2025).

[439] ضوابط إجراءات الإثبات إلكترونياً [решение Министра юстиции КСА № 921 от 12.10.2022 «Контроль процедур электронного доказательства»] // Министерство юстиции КСА. URL: https://laws.moj.gov.sa/legislation/ps6CWt8A6oJ1b6j+n6vr%2Fw== (дата обращения: 19.03.2025).

[440] В Рекомендациях Верховного народного суда КНР № 11, направленные на предупреждение и исправление судебных ошибок в уголовных делах, от 2013 г. указывалось, что не может иметь место приобщение предметов или средств в качестве доказательств без опознания, экспертизы или определения происхождения другим способом. См. подробнее Васюков В.Ф., Старжинская А.Н. К вопросу об организационных и процессуальных особенностях получения электронных данных при расследовании преступлений (опыт Китайской Народной Республики) // Вестник Московского университета МВД России. 2024. № 6. С. 20-25.

Франкоязычные исследователи стран аль-Магриба отмечают допустимость подобных доказательств в случаях соблюдения общих принципов (представление в ходе судебного разбирательства и их обсуждение)[441].

В арабоязычной юридической литературе принято считать, что если изъят материальный носитель информации с электронными данными, то он должен признаваться в качестве вещественного доказательства[442].

Согласно Положению КСА 2022 г., под цифровыми доказательствами понимаются любые данные, созданные, выпущенные, полученные, хранящиеся или сообщаемые с помощью цифровых средств, которые можно восстановить или получить понятным образом. В ст. 65 ФДЗ ОАЭ №34-2021 и ст. 11 Закона АРЕ № 175-2018 уточняются источники цифровых доказательств — доказательства, полученные или извлеченные из электронных устройств, оборудования, носителей информации или приводов, электронных носителей, информационных систем, компьютерных программ, программного обеспечения или из любого информационно-технологического оборудования / ИТ.

В п. 8 ст. 2 Прокламации ФДРЭ № 652/2009 от 28.08.2009 «О борьбе с терроризмом»[443] отличительными признаками цифровых доказательств являются хранение или передача информации в цифровой форме, которая записывается или хранится в любом пространстве или с помощью компьютерной системы или сходного устройства; возможность прочитать или воспринять лицом, компьютерной системой или иным сходным устройством; включение дисплея, распечатку или выход данных.

Электронные доказательства и их источники можно классифицировать, исходя из нормативных и доктринальных начал. Теоретически цифровые доказательства можно поделить на несколько групп: связанные с компьютерами, с

---

[441] См., например, El Jaouad A.A. La Preuve Numerique A L'epreuve De La Cybercriminalite En Droit Marocain // Revue droit & société. 2023. № 11. P. 7–18.

[442] الحوامدة، لورانس. حجيَّة الأدلة الرقميَّة في الإثبات الجنائيّ: دراسة تحليليَّة مُقارنة // مجلة البحوث الفقهيَّة والقانونيَّة. ٢٠٢١. ٣٦. ٨٨٣-٩٣٦ ص. [Аль-Хавамдех Л. Допустимость цифровых доказательств в уголовном судопроизводстве: Сравнительное аналитическое исследование // Журнал юриспруденции и правовых исследований. 2021. № 36. С. 883–936].

[443] Anti-Terrorism Proclamation No. 652/2009 // Federal Negarit Gazeta. 2009. № 47. P. 4827–4842.

Интернетом и иными сетями, а также с протоколами обмена информацией между устройствами[444]. При этом в основном следы делят на активные и пассивные[445].

Практически понятием «электронные доказательства» (оригиналы и копии) охватываются электронные документы и сертификаты, цифровые / электронные записи (араб. «السجل الرقمي» / «السجلات الإلكترونية»)[446]; цифровой / электронный контент или каталог (араб. «المحرَّر الرقمي» / «المحرر الإلكتروني»)[447]; электронная / цифровая подпись (араб. «التوقيع الرقمي»); цифровая корреспонденция, включая переписку на электронных почтовых ящиках и в социальных сетях (араб. « المراسلات الرقمية بما فيها البريد الرقمي» / «البريد الإلكتروني»); средства связи (араб. «وسائل الاتصال»); цифровые / электронные средства (араб. «الوسائط الرقمية» / «الوسائط الإلكترونية»)[448]; иные — любые электронные доказательства, соответствующие исполнительным регламентам, или иное цифровое средство, которое позволяет представить доказательства и при необходимости их проверить.

Процедурным руководством к Положению КСА 2022 г. от 12.10.2022[449] определены общедоступные цифровые носители (любые средства, которые были доступны для общего использования или для клиентов с особым типом сделок) и

---

444 الهمداني ميسون خلف حمد الحمداني. مشروعية الدليل الإلكتروني كدليل في القضايا الجنائية // مجلة كلية الحقوق لجامعة النهرين. ٢٠١٦. ١٨. ٢. ١٩٥-٢٥٤ ص. [Аль-Хамдани Мэйсун Халаф Хамад. Законность электронных доказательств в качестве доказательств по уголовному делу // Журнал колледжа права Университета Аль-Нахрэйн. 2016. № 18 (2). С. 195–254].

445 El-Kady R.M. Handling E-evidence in Egyptian and Comparative Legislation: A Comparative Analytical Study // Arab Journal of Forensic Sciences and Forensic Medicine. 2023. № 5 (2). P. 191–222.

446 Электронная запись фактически является задокументированным свидетельством любого цифрового перемещения.

447 Источник, сохраняемый и распространяемый изначально в электронном виде.

448 Программы, которые объединяют группу медиа, то есть звук, изображение, движение, текст, рисунок. См. подробнее لد الصديق ميلود. الوسائط الرقمية الحديثة من شبكات التواصل الاجتماعي // مجلة أكاديميا. ٢٠١٦. ٤. ١٩٣-٢١١ [Сиддик Милуд. Современные цифровые медиа из социальных сетей // Академический журнал. 2016. № 4. С. 193-211].

449 الأدلة الإجرائية لنظام الإثبات [Процедурные руководства к Положению о доказательствах КСА от 12.10.2022] // Министерство юстиции КСА. URL: https://laws.moj.gov.sa/legislation/8ST%2Fur3URoFaiLSA0IAGGw==#content-card-VeTqvtWGcIOGGQvMXQ (дата обращения: 25.03.2025).

задокументованные цифровые средства (любые средства, лицензированные компетентным органом, которые были предоставлены клиентам)[450].

Согласно п. 8 ч. 2 ст. 50 уголовно-процессуального закона КНР[451] и ст. 65 Уголовно-процессуальных правил Верховной Народной прокуратуры КНР от 30.12.2019[452], выделяются электронные данные (кит. «电子 数据», «Diànzǐ shùjù») и аудиовизуальные материалы (кит. «视听 资料», «Shìtīng zīliào»). К первой категории относятся данные, которые формируются при возникновении дела, хранятся, обрабатываются и передаются в цифровой форме и могут доказывать обстоятельства дела:

- информация, опубликованная на веб-страницах, в блогах, микроблогах, Moments, Tieba, сетевых дисках, социальных платформах, форумах и других онлайн-платформах;

- коммуникационная информация из текстовых сообщений мобильного телефона, электронной почты, сервиса обмена мгновенными сообщениями, групп связи и других служб сетевых приложений;

- информация о регистрации пользователя, информация для аутентификации личности, цифровая подпись, биометрическая информация (идентификационные данные);

- информация о поведении пользователя (записи электронных транзакций, записи связи, записи просмотра, записи операций, установка программы, операции, записи об удалении и т.д.);

---

[450] Волеводз А.Г., Цыплакова А.Д. Цифровые доказательства в уголовном процессе государств-членов Совета сотрудничества арабских государств Персидского залива: правовой статус и процедуры // Вестник экономической безопасности. 2024. № 2. С. 21–29.

[451] 中华人民共和国刑事诉讼法 [Уголовно-процессуальный закон Китайской Народной Республики] // Портал центрального правительства. Законы и нормативные акты. URL: https://www.gov.cn/flfg/2012-03/17/content_2094354.htm (Дата обращения: 21.10.2024).

[452] 人民检察院刑事诉讼规则 [Уголовно-процессуальные правила Верховной Народной прокуратуры от 30.12.2019] // Онлайн-законодательство Верховной народной прокуратуры. URL: https://www.spp.gov.cn/spp/xwfbh/wsfbh/201912/t20191230_451490.shtml#1 (дата обращения: 21.10.2024).

- сведения о поведенческих инструментах: вредоносные программы, инструментальное программное обеспечение, исходный код веб-сайта, запущенные скрипты и т.д.;

- документы, изображения, аудио и видео, цифровые сертификаты, файлы баз данных, компьютерные программы и другие электронные файлы с учётом времени их создания, доступа, изменения, размера и других метаданных (ст. 27 уведомления ВНП КНР 2021 г.).

С одной стороны, согласно Закону Республики Индия № 1 от 15.03.1872 «Об индийских доказательствах» (ред. от 13.03.2020)[453], доказательства могут быть устными или документарными. К последним относят и электронные, и цифровые записи. С другой — согласно разделу 79А Закона РИ № 21-2000, любая информация, имеющая доказательную ценность, которая хранится или передается в электронной форме, является электронной формой доказательства и включает в себя компьютерные доказательства (англ. «computer evidence»), цифровое аудио, цифровое видео, мобильные телефоны, цифровые факсимильные аппараты. Для целей признания в качестве доказательства в любом суде или ином органе назначается исследователь (англ. «Examiner of Electronic Evidence») в статусе эксперта. К таковым относят Центральную судебно-медицинскую лабораторию (Хайдарабад при Управлении судебно-медицинских служб МВД), Управление судебно-медицинских наук (Гандинагар, штат Гуджарат), Лабораторию компьютерной судебной экспертизы и интеллектуального анализа данных в рамках Управления по расследованию серьезного мошенничества Министерства корпоративных дел (Нью-Дели), Лабораторию судебной экспертизы (Рохини, Нью-Дели), Лабораторию киберэкспертизы Кибергруппы Главного управления военных операций, государственную лабораторию судебно-медицинской экспертизы (Мадивала, Бангалуру) при Директории судебно-медицинской экспертизы Департамента полиции (Карнатака), Лабораторию киберэкспертизы Кибергруппы

[453] Indian Evidence Act, 1872 // Digital Repository of Laws. URL: https://www.indiacode.nic.in/bitstream/123456789/15351/1/iea_1872.pdf (accessed 19.03.2025).

BBC (Нью-Дели). Согласно разделу 65B Закона Республики Индия № 1 «О доказательствах» от 1872 г. предусмотрена подробная процедура.

Согласно указу министра юстиции ОАЭ № 259 от 27.03.2019 «Относительно процедурного руководства по организации судебного разбирательства с использованием электронных средств и удаленной связи в уголовном судопроизводстве» [454], использование электронных документов и электронной подписи в качестве доказательств при соблюдении условий Федерального закона ОАЭ № 1 от 2006 г. «Об электронных сделках и торговле»[455]. Однако с принятием нового уголовно-процессуального закона и ФДЗ ОАЭ № 34-2021 данный указ утратил силу.

Существует три мнения по поводу их правового статуса: цифровые доказательства имеют абсолютную доказательственную силу; они указывают лишь на факт использования компьютера, но не вину, поскольку аккаунт обвиняемого может быть взломан или скомпрометирован; решение о принятии остаётся в дискреции суда[456].

Исторически принятие электронных доказательств было действительно на усмотрение судьи, особенно в арабских странах. Своё убеждение в чём-либо судья должен черпать из источников, которые представлены перед ним устно, и следует принципу свободной оценки доказательств (араб. «نظام الإثبات الحر»), пока он не убеждён в виновности лица (с араб. «نظام الاقتناع الذاتي» дословно — система самоубеждения). Например, в Султанате Оман при оценке доказательств придерживаются следующего подхода: «*достаточно судить о невиновности*

---

[454] قرار وزاري رقم ٢٥٩ صادر بتاريخ ٢٧.٠٩.٢٠١٩ في شأن الدليل الإجرائي لتنظيم التقاضي باستخدام الوسائل الالكترونية والاتصال عن بعد في الاجراءات الجزائية [указ министра юстиции ОАЭ № 259 от 27.03.2019 «Относительно процедурного руководства по организации судебного разбирательства с использованием электронных средств и удаленной связи в уголовном судопроизводстве»] // Официальная база законодательства ОАЭ. URL: https://elaws.moj.gov.ae/UAE-MOJ_LC-Ar/00_جزائية%20اجراءات/UAE-LC-Ar_2019-03-27_00259_Karwi.html?val=AL1 (дата обращения: 25.03.2025).

[455] قانون اتحادي رقم ١ لسنة ٢٠٠٦م في شأن المعاملات والتجارة الإلكترونية [Федеральный закон ОАЭ № 1 от 2006 г. «Об электронных сделках и торговле»] // Официальная база законодательства ОАЭ. URL: https://elaws.moj.gov.ae/UAE-MOJ_OG/10002S_2006/01-31-2006_0442/UAE-OG_2006-01-30_00001_kait.pdf (дата обращения: 25.03.2025).

[456] El-Kady R. Указ. Соч.

только по обоснованному сомнению в обоснованности приписывания обвинения обвиняемому или при недостаточности доказательств, ибо основной принцип в человеке — невиновность, а преступление — форма девиантного поведения, выходящего за рамки обычного» (решение Верховного суда Султаната Оман № 50 от 02.03.2004 по апелляции №22/2004). Подобный подход прочно укоренился в судебной практике арабских стран. Например, в решении Генеральной Ассамблеи Верховного суда КСА № 34 от 11.01.2018 указывается: «*цифровые доказательства являются действительными, если они свободны от непредвиденных обстоятельств. Они различаются по силе в зависимости от инцидента, его обстоятельств и сведений, которые они подтверждают*»[457].

В решении Федерального Верховного суда ОАЭ № 1468 от 25.04.2023: «*судья по уголовным делам пользуется полной свободой для принятия решения с опорой не только на законодательство и исламский шариат и формирует своё убеждение на основе устных или технических доказательств или доводов. При формировании своего убеждения он опирается на правильную картину фактов дела и связанных с ним юридических фактов из всех элементов, представленных путем дедукции и индукции*» [458].

В решении Верховного суда АНДР № 1091284 от 13.01.2022: «*законодатель, установив, что преступления могут быть доказаны любым методом доказывания, не сделал это в абсолютном порядке, а ограничил свободу судей первой инстанции в построении собственного убеждения, ограничив аргументацию без установления каких-либо пределов*»[459].

---

[457] قرار الهيئة العامة للمحكمة العليا رقم (٣٤) وتاريخ ٢٤-٠٤-١٤٣٩هـ [Решение Генеральной Ассамблеи Верховного суда № 34 от 24.04.1439] // Юридическая контора Аль-Мухтара. URL: https://elmokhtarlaw.com/3-رقم-العليا-للمحكمة-العامة-الهيئة-قرار/ (дата обращения: 19.03.2025).

[458] الطعن رقم ١٤٦٨ لسنة ٢٠٢٢ صادر بتاريخ ٢٠٢٣/٠٤/٢٥ [Апелляция No 1468 от 2022 года, по которой принято решение от 25.04.2023] // Официальная база законодательства ОАЭ. URL: https://elaws.moj.gov.ae/UAE-MOJ_CP-Ar/00_2023/00_الجزائية%20الاحكام/UAE-CP-Ar_2023-04-25_01468_Taan.html (дата обращения: 19.03.2025).

[459] ملف رقم: 1091284 قرار بتاريخ: 2022.01.13 [Номер файла: 1091284 Решение: 13.01.2022] // Верховный суд АНДР: официальный сайт. URL: https://www.coursupreme.dz/-قرار-1091284-رقم-ملف/الغرف-الجزائية/من-قرارات-المحكمة-العليا-بتاريخ-20220113 (дата обращения: 19.03.2025).

Электронное доказательство должно отвечать минимальным критериям: «*если компьютерные данные были созданы, обработаны, сохранены или переданы третьей стороной… и соответствующая компьютерная или телекоммуникационная система функционирует таким образом, что не ставит под угрозу точность, целостность, действительность и не отрицает данные*»[460] (ИРИ); «*любой документ / заверенная копия документа / заверенная распечатка любой электронной записи, относящейся к компьютерным данным, изъятым на законных основаниях, могут быть представлены в качестве доказательства в ходе судебного разбирательства и являются допустимыми*» (ФДРЭ). Среди принципов, обязательных к соблюдению в арабских странах, стоит выделить также законность (араб. «شرعية» или «قانونية»), свобода доступа к доказательствам и правомерности данного доступа, определённость (араб. «يقينية»), обсуждение (араб. «مشروعية»), принятие (араб. «قبول»), достоверность или надёжность (араб. «مصداقية»), повторяемость (араб. «تكرار»), целостность (араб. «سلامة»), причинная связь (дословно с араб. «سبب و مسبب» причина и являющееся причиной) и документирование (араб. «توثيق»).

Источниками могут выступать история поиска в веб-браузере, облачное хранилище, записи звонков и сообщений, профили, посты и беседы в социальных сетях, на форумах, камеры видеонаблюдения, содержимое электронных устройств, данные геолокации, полученные на основе сетевой активности пользователя[461].

С точки зрения **процессуального оформления и порядка сбора и хранения** электронных доказательств объём регламентации разнится от страны к стране, что

---

[460] На необходимость соблюдения принципов полноты, целостности, достоверности и неопровержимости, а также соблюдение механизмов безопасности указывает ст. 655 уголовно-процессуального закона от 24.02.2014 ИРИ, ст. 12 Закона ИРИ от 01.07.2004 «Об электронной коммерции». См. подробнее قانون آیین دادرسی کیفری [Уголовно-процессуальный закон] // Законодательная база ИРИ. URL: http://dotic.ir/news/5584/قانون-آیین-دادرسي-کیفري (дата обращения: 19.03.2025) и قانون تجارت الکترونیکی [Закон «Об электронной коммерции»] // Исследовательский центр Исламского совета ИРИ. URL: https://rc.majlis.ir/fa/law/show/93997 (дата обращения: 19.03.2025).

[461] El-Kady R. The Authenticity of Digital Evidence Before Criminal Courts // ResearchGate. 01.2024. URL: https://www.researchgate.net/publication/377527331_The_Authenticity_of_Digital_Evidence_Before_Criminal_Courts (accessed 01.05.2025) (in Arabic).

будет рассмотрено по порядку, однако отметим, что более подробным регулированием характеризуется Иран и КНР.

Основным следственным действием является контроль, обыск, выемка, сбор или конфискация данных, информации или информационных систем или отслеживание их до любого места, системы, программы, электронного носителя или компьютера; поиск, проверка, вход и доступ к компьютерным программам, базам данных, информационным устройствам и системам для достижения цели контроля, что в последующем оформляется соответствующим протоколом — *тафтиишун* (араб. «تفتيش») или *тäфтиш и тоугиф* (перс. «تفتيش و توقيف»)[462]. Целью *тафтиишун* является получение и овладение/изъятие любого предмета, связанного с преступлением[463]. Порядок осуществления указанного следственного действия в арабских странах и ИРИ разнится. Эмиратский прокурор уполномочен производить выемку предметов, документов, корреспонденции, писем, газет, печатных изданий, посылок, телеграмм, осмотр устройств, сетей, оборудования, носителей информации, электронных средств, информационных систем, компьютерных программ или технических средств с привлечением при необходимости экспертов или специалистов (ст. ст. 70, 73 Федерального декрета-закона ОАЭ № 38 от 30.10.2022 «Об уголовных мерах»[464]). На перечисленные действия в части выемок в КСА требуется решение Председателя Бюро расследований и государственной прокуратуры (ст. ст. 56–59 Положения КСА 2013 г.[465]). Преступления против АСОД в АНДР относятся к категории деяний, по которым допускается производство следственным судьей[466] в любое время дня и ночи осмотр, обыск и выемка в любых

---

[462] Подчиняется общему порядку, предусмотренному уголовно-процессуальным законом.

[463] Algabri Z.A.N., Abdul Shukor S., Mohammed Hasan B.M. Evidence and investigation of Internet crimes in UAE // Al-Hikmah: International Journal of Islamic Studies and Human Sciences. 2022. № 5 (2). P. 236.

[464] مرسوم بقانون اتحادي رقم (38) لسنة 2022 بإصدار قانون الإجراءات الجزائية [Федеральный декрет-закон ОАЭ № 38 от 2022 года «Об уголовных мерах»] // Официальная база законодательства ОАЭ. URL: https://www.uaelegislation.gov.ae/en/legislations/1609 (дата обращения: 01.04.2025).

[465] نظام الإجراءات الجزائية [Положение КСА от 12.06.2013 «Об уголовных мерах»] // Бюро экспертов Совета министров Королевства Саудовская Аравия. URL: https://laws.boe.gov.sa/BoeLaws/Laws/LawDetails/8f1b7079-a5f0-425d-b5e0-a9a700f26b2d/1 (дата обращения: 01.04.2025).

[466] Он может поручить выполнить это и судебной полиции. Нужно также понимать, что в АНДР, как и в других странах аль-Магриба, велико влияние французского наследия.

жилых и нежилых помещениях на всей территории государства на основании разрешения компетентного прокурора (ст. 47 Закона АНДР от 08.06.1966 в ред. от 28.12.2021 «Об уголовных мерах» [467]).

В Катаре порядок кардинально отличается: в случае расследования преступлений отдельных видов[468] достаточно разрешения Генерального прокурора, в остальных же случаях требуется судебное решение за исключением случаев, когда производится осмотр в присутствии обвиняемого, лица, у которого находятся перечисленные предметы либо которому были отправлены [469] . Каирский апелляционный суд по экономическим преступлениям указал, что для изъятия компьютера, использованного при совершении преступления, не требуется разрешения окружного судьи. Вдобавок электронные сообщения могут изыматься по решению прокуратуры в отличие от проверки писем и посылок в почтовых отделениях и контроля и записи (без)проводных разговоров[470]. Это отличается от подхода, определённого в Законе САР Макао № 11 от 26.06.2009 «О компьютерных преступлениях» (в ред. 2020 г.), который отсылает к положениям уголовно-процессуального закона САР Макао[471] о получении судебного разрешения (ст. ст. 164 и 235).

Изъятие компьютерных или телекоммуникационных данных или систем в ИРИ производится на основании судебного решения. Изъятие систем осуществляется в следующих случаях:

- хранимые данные труднодоступны или имеют большой объём;

---

[467] Указ № 66-156 от 18.02.1386 (хиджра), что соответствует 08.06.1966, включающий в себя измененный и дополненный уголовный закон [الأمر رقم ٦٦-١٥٦ المؤرخ في ١٨ صفر عام ١٣٨٦ الموافق لـ ٨يونيو سنة ١٩٦٦ يتضمن قانون العقوبات المعدل والمتمم] // Поисковая система алжирского права. URL: https://legisdz.com/ar/LawTexts/alamr-rqm-66-156-almwrkh-fy-18-sfr-am-1386-almwafq-l8ywnyw-snt-1966-ytdmn-qanwn-alqwbat (дата обращения: 25.01.2025).

[468] Деяния, направленные против внутренней или внешней безопасности государства, нарушения антинаркотического регулирования и закона об оружии, боеприпасах и взрывчатых веществах.

[469] Цыплакова А.Д. Должностные лица и органы, обеспечивающие реализацию полноты судебной власти, в арабских государствах: понятие и полномочия // Вестник Дальневосточного юридического института МВД России имени И.Ф. Шилова. 2025. № 2 (71). С. 142-151.

[470] El-Kady R. Указ. Соч.

[471] 刑事訴訟法典 [Уголовно-процессуальный закон] // Законодательная база Макао. URL: https://bo.io.gov.mo/bo/i/96/36/codpropencn/codpropen0001.asp#a164 (дата обращения: 06.06.2025).

- аудит и анализ данных невозможен без аппаратной системы;

- законный владелец системы дал согласие;

- сбор данных технически невозможен;

- проверка на месте приводит к повреждению данных (ст. 676 Уголовно-процессуального закона ИРИ от 03.07.2013).

При этом возникают трудности с обязанностью раскрывать информацию или секреты доступа к электронным средствам частными лицами ввиду принципа неприкосновенности частной жизни. Если это касается обвиняемого, то он пользуется правом хранить молчание и не может быть принужден к раскрытию ключей доступа к системам электронных средств или к распечатке файлов или данных, хранящихся в этих системах. Иные лица, например операторы компьютеров, эксперты по программированию, аналитики, инженеры по обслуживанию и связи, а также теоретические менеджеры выступают в качестве свидетелей или специалистов, а потому закон налагает на них юридическое обязательство раскрыть коды, пароли, программы или лазейки, используемые для входа в системы, а также содействовать в получении доступа, раскрытии, переносе или сохранении данных для целей расследования[472]. Они могут рассматриваться в качестве свидетелей с процессуальной точки зрения. Юридические лица могут быть объектами проверки (местом осмотра или обыска) [473] . Любое здание, транспортное средство, судно, самолёт или место, в котором, по мнению должного лица, хранится или скрывается любые несанкционированные телекоммуникационные сети, оборудование или радиооборудование, в отношении которых было совершено преступление, подлежит обыску по разделу 43 Закона РИ № 44 от 24.12.2023 «О телекоммуникациях». Любая информация, документ или

---

[472] В судебной практике однозначно решается вопрос об отказе или воздержании от ответа. См. подробней Аль-Махмуд Али Хамудату. Доказательства киберпреступлений, умысел и оценка в рамках теории доказательств по уголовным делам // Журнал безопасности и права. 2003. № 1. С. 9–95 (на араб. яз.) С. 46–47; Хишам Мухаммад Харид Растум. Информационные преступления: истоки технического уголовного расследования / Конференция по исследованию права, компьютеров и Интернета в сотрудничестве с Центром стратегических исследований и разработок Эмиратов и Центром информационных технологий при университете: сборник. Аль-Айн: Университет ОАЭ. Колледж шариата и права, 2004. 1145 с. (на араб. яз.) С. 77–88.

[473] Там же. С. 55.

запись, находящаяся во владении или под контролем любой уполномоченной организации или правопреемника, относящаяся к телекоммуникационной услуге, сети или использованию спектра, предоставляемой организацией, потребителем или абонентом, должна быть предоставлена в связи с расследованием по письменному распоряжению уполномоченным центральным правительством должностным лицом (раздел 44 Закона РИ № 44-2023).

Лица, которые контролируют или владеют данными, компьютерными или телекоммуникационными системами, обязаны сотрудничать в исполнении постановления о проведении обыска и выемки. Если осмотр или выемка невозможны из-за отсутствия сотрудничества или отсутствия доступа к этим лицам, способ доступа к данным или системам (e.g., проникновение на объект, устранение препятствий для использования оборудования и программного обеспечения, расшифровка) будет определяться постановлением судебного органа (ст. 31 Постановления Главы судебной власти ИРИ).

В главе 2 Закона Бахрейна № 60-2014, как и в указанном Постановлении Главы судебной власти ИРИ, Исполнительных правилах к Закону АРЕ № 175-2018, Законе САР Макао № 11 от 26.06.2009 «О компьютерных преступлениях» (в ред. 2020 г.) подобная проблема решена через приказы прокуратуры или судебные постановления[474], однако сроки различаются.

Так, например, бахрейновская прокуратура может издать приказ любому лицу поддерживать целостность определённых данных ИТ, включая данные о трафике, хранящиеся в системе информационных технологий, находящихся в его распоряжении или под его контролем, в случае наличия доказательств, что такие данные могут быть утеряны или изменены. Лицо обязано сохранить данные и их целостность в течение периода, не превышающего 90 дней, а Высокий уголовный суд Королевства Бахрейн может уполномочить публичное обвинение, по запросу, сопровождаемому обоснованиями, представленными за три дня до истечения указанного периода, продлить срок, не превышающий в общей сложности ещё на

[474] В Макао исключительно судебный порядок.

90 дней. Прокуратура также может распорядиться сохранить конфиденциальность приказа. Она может издать приказ лицу, которое владеет определенными данными или контролирует их, незамедлительно представить их, включая данные, хранящиеся в ИТ-системе или любом ином ИТ-средстве; любому поставщику услуг предоставить любую информацию, находящуюся в его распоряжении или под его контролем, о любом абоненте или пользователе своих услуг, независимо от того, является ли такая информация в форме данных ИТ или в любой другой форме и не включает данные траффика и контента.

Бахрейновская прокуратура может издать приказ о вводе/входе (араб. «أمرا مسببا بالدخول») с целью проверки ИТ-системы, связанной с преступлением или любым его элементом, а также любых хранящихся в ней данных об ИТ-среде, любого из средств хранения данных ИТ, на котором, вероятно, будут храниться данные, связанные с преступлением. Если прокуратура имеет веские основания полагать, что данные, связанные с преступлением, хранятся в другой ИТ-системе или ее части, и такие данные могут быть доступны через первую ИТ-систему или юридически доступны через неё, прокуратура может издать мотивированное постановление о расширении доступа и проверки/инспекции другой системы. При проверке/инспекции государственное обвинение имеет право изымать и сохранять данные ИТ-средств, включая следующее:

1) контроль и сохранение ИТ-системы, или любой ее части, или любого из носителей данных ИТ-средств;

2) воспроизведение данных ИТ-средств и сохранение копии;

3) поддержание целостности данных ИТ-средств;

4) загрузка данных ИТ-инструмента из ИТ-системы, которая была доступна или сделала доступ к ней невозможным.

Суд первой инстанции Королевства Бахрейн может по ходатайству государственного обвинения и после рассмотрения документов распорядиться о следующем:

1) оперативном сохранении данных о трафике, связанные с преступлением, независимо от того, транслировалась ли передача через одного или нескольких поставщиков услуг;

2) раскрытии достаточного количества маршрутных данных, чтобы государственное обвинение могло определить поставщика услуг и маршрут, по которому были отправлены эти данные, если это способствует раскрытию истине (ст. 14).

Для осуществления п. 2 ст. 14 Закона Бахрейн № 60-2014 прокуратура может назначить любое лицо, компетентное собирать и записывать данные маршрута и/или данные о его содержании с указанием конкретных сообщений, отправляемых ИТ-системой, когда происходят такие сообщения; любого поставщика услуг для выполнения упомянутых работ или для оказания необходимой помощи тем, кому поручено прокуратурой выполнение этих задач; поручить любому компетентному лицу заблокировать данные о содержании любых ИТ-средств или любой их части, с помощью которых было совершено преступление в области информационных технологий. Разрешение действует на срок, не превышающий 30 дней, с возможностью продления на один или несколько аналогичных периодов[475].

Более того, судья первой инстанции может по ходатайству прокуратуры и после рассмотрения документов издать решение о приказе любому лицу, компетентному или знакомому с тем, как работает ИТ-система и мерами, применяемым для защиты данных, хранящихся в этой системе, предоставить ей, в разумной степени, информацию, необходимую для осуществления процедур, предусмотренных в ст. ст. 15 и 16 Закона Бахрейна № 60-2014[476].

Положения иранского законодательства также предусматривает прослушивание контента компьютерного общения (перс. « شنود محتوای ارتباطات رایانه

[475] В АРЕ возможно только один раз продление срока в отличие от Бахрейна.

[476] Collecting Electronic Evidence in Criminal Cases in Russia and Foreign Countries: Experiences and Problems: Monograph / editors S.P. Shcherba (Russian ed.) and P.A. Litvishko (English ed.). Moscow: Publishing House “Gorodets”, 2024. 224 p. Chapter 1. The Concept and General Characteristics of Electronic Evidence in Criminal Proceedings (E.A. Arkhipova, E.V. Bykova, S.P. Shcherba, P.A. Smirnov, A.D. Tsyplakova and A.G. Volevodz). P. 31-37.

ای»): «*Прослушивание*[477] *содержания непубличных сообщений в компьютерных или телекоммуникационных системах должно осуществляться в соответствии с положениями, касающимися перехвата телефонных разговоров. Доступ к содержимому сохраненных закрытых сообщений, таких как электронная почта или текстовые сообщения, осуществляется при условии прослушивания и соблюдения соответствующих правил*» (ст. 48 Закона ИРИ 2009 г.).

В АНДР электронный мониторинг (араб. «المراقبة الإلكترونية»)[478] как оперативное использование технических средств наблюдения за электронными сообщениями выделен в качестве отдельного метода расследования в следующих случаях:

- при совершении преступлений террористической направленности, а равно деяний, направленных против государственной безопасности;

- при наличии сведений о том, что готовящаяся атака угрожает общественным интересам, национальной обороне, государственным учреждениям или национальной экономике;

- при невозможности достижения результата при расследовании и судебном разбирательстве без использования подобного метода;

- при осуществлении запросов о взаимной правовой помощи [по уголовным делам].

Согласно Постановлению Главы судебной власти ИРИ, поставщики Интернет-услуг должны фиксировать данные пользователя, адрес, время начала и окончания подключения, а также присвоенный IP-адрес и данные о трафике в течение не менее 6 месяцев после прекращения подписки или расторжения пользовательского договора в соответствии с официальным календарём и временем страны (солнечная хиджра). Поставщики услуг хостинга обязаны хранить данные

---

[477] Это относится к любому доступу к контенту, передаваемому в закрытых коммуникациях в компьютерных или телекоммуникационных системах или с использованием электромагнитных волн с использованием соответствующих аппаратных и программных систем и оборудования.

[478] Обратим внимание, что электронный мониторинг в ОАЭ — это мера процессуального принуждения. См. Цыплакова А.Д. Должностные лица и органы, обеспечивающие реализацию полноты судебной власти, в арабских государствах: понятие и полномочия // Вестник Дальневосточного юридического института МВД России имени И.Ф. Шилова. 2025. № 2 (71). С. 142-151.

своих пользователей в течение не менее 6 месяцев после прекращения подписки, а также сохраненный контент и данные о трафике, возникшие в результате внесенных изменений, не менее 15 дней. Уполномоченный на расследование орган может распорядиться о защите любого типа хранящихся компьютерных данных, включая зашифрованные, удаленные, скрытые, сжатые или утаенные данные, а также данные, тип и название которых временно изменены, или данные, для проверки которых требуется специальное оборудование. Поставщик услуг сохраняет указанные сведения и исполняет охранный приказ (перс. «دستور حفاظت») вплоть до вынесения судебного решения с уведомлением судебного органа в течение 24 часов. Срок защиты данных в подобном случае составляет до 3-х месяцев с возможностью продления.

В целях сохранения первоначального состояния доказательств и предотвращения их изменения, искажения или повреждения судебный орган устанавливает срок их хранения до 5 дней. Если требуется более длительный период хранения, то указанный выше период может быть мотивированно продлен. В соответствующих случаях исполнение охранного приказа осуществляется под надзором специализированных должностных лиц или доверенных экспертов.

Предоставление данных осуществляется путём предоставления распечатанной копии данных / компьютерной (электронной) версии данных[479] или доступа к данным, а равно путём передачи компьютерного и телекоммуникационного оборудования. При этом подготавливается протокол-отчёт (перс. «صورت جلسه») в 3-х экземплярах для судебного органа, поставщика и непосредственного получателя (органа, осуществляющего расследование) с указанием следующих сведений: номер и дата судебного постановления о предоставлении данных, сведения о поставщике и получателе, время и место, тип и объём данных, информация о порядке обработки и хранения данных, меры безопасности, технические характеристики оборудования и программного обеспечения, метод представления и спецификация данных.

---

[479] Копии, сделанные с компьютерных данных, могут использоваться в форме текста, аудио или изображений в качестве исходных данных.

Отказ от исполнения перечисленных судебных решений и охранных приказов может повлечь за собой уголовную ответственность, что характерно не только для Ирана, но и для других азиатских стран, в частности КНР и её САР[480].

При этом изъятие или перехват данных может сопровождаться использованием методов недоступности (смена паролей или шифрование). Постановление об изъятии системы не распространяется на другое оборудование или носители данных, подключенные к ней, если иное не указано в приказе.

При этом в Катаре предусмотрены иные сроки хранения: информация о пользователях — в течение 1 года; данные о ИТ — не менее 120 дней; временное и срочное хранение данных информационных технологий, данных о трафике или контент — в течение 90 дней, возобновляемое по запросу компетентного органа или следственных и судебных органов.

В Тунисской Республике есть лишь минимальный порог в два года с даты регистрации, а сам срок в зависимости от типа данных определяется совместным решением министра национальной обороны, министра внутренних дел, министра юстиции и министра, ответственного за связь. Сохраняемые данные охватывают данные: которые позволяют идентифицировать пользователей сервиса; связанные с коммуникационным трафиком; связанные с периферийными устройствами связи; связанные с географическим местоположением пользователя; о доступности и использовании защищённого контента.

Поставщики услуг в АНДР и ФДРЭ хранят с момента регистрации пользователя год сведения о трафике. К ним относят:

- данные, позволяющие идентифицировать пользователей услуг;

- сведения, относящиеся к конечному оборудованию, используемому для подключения;

- технические характеристики, дата, время и продолжительность соединения;

---

[480] Ст. 16 Закона САР Макао № 11 от 26.06.2009 «О компьютерных преступлениях» (в ред. 2020 года) отсылает к ст. 312 уголовного закона САР Макао. 刑法典 [Уголовный закон] // Законодательная база Макао. URL: https://bo.io.gov.mo/bo/i/95/46/codpencn/codpen0001.asp#l2a128 (дата обращения: 06.06.2025).

- информация, относящаяся к запрашиваемым или используемым дополнительным услугам и их поставщикам;

- данные, позволяющие определить адресата или адресатов сообщения, Интернет-ресурсы, к которым осуществлялся доступ;

- сведения, позволяющие идентифицировать и определить местонахождение источника звонка (ст. 11 Закона АНДР № 09-04).

Храниться также может и учёт преобразования частных сетевых адресов в публичные сети (англ. «NAT») в течение 1 года, согласно ст. 16А Закона САР Макао № 11 от 26.06.2009 «О компьютерных преступлениях» (в ред. 2020 года).

Исходя из устойчивой судебной практики (решение Кассационного суда Эмирата Дубай от 02.08.2019 по апелляции № 13/2010 и практика Кассационного суда Каира 2014–2020 гг., практика Федерального Верховного суда ОАЭ 2022–2024 гг.), записи о посещениях веб-сайтов, журналы и таблицы рабочего состояния с доступом к адресам промежуточного, основного или сервисного компьютеров могут как фиксироваться с помощью данных поставщиков услуг, так и устанавливаться экспертом[481]. Записи могут также производиться и фиксироваться следователями на компакт-диски (практика Кассационного суда Каира по делам о поджоге научного комплекса и взяточничестве в 1996 г.)[482].

В качестве цифровых доказательств в судебной практике Верховного суда Республики Индия принимались электронная статистика при наличии сертификата, письма с электронного почтового ящика, цифровые документы (дело Анвар П.В. против П.К. Башир и другие 2014 г.), отчёты экспертов-криминалистов в виртуальной сфере (Штат Махараштра против Доктора Прафулл Б. Десай 2003 г.), перехват телефонных переговоров (Штат NCT Дели против Навджот Сандху 2005 г.)[483].

---

[481] حجية الدليل الالكتروني في الاثبات الجنائي وسمطة القاضي في تقديره. محمود صبحي محمد محمود ا زيد [Махмуд Собхи Мухаммад Махмуд Заид. Авторитетность электронных доказательств в уголовном деле и дискреционные полномочия судьи] // Журнал гуманитарных наук Бехна. 2022. № 1 (2). С. 27–48.
[482] El-Kady R. Указ. Соч.
[483] Patil H.B., Chowbe A. Указ. Соч.

Примечательно, что в ФДРЭ перехват контента или наблюдение может осуществляться без судебного решения с разрешения Министра, а в Тунисе — прокурора Республики или следственного судьи.

Согласно Правилам сбора электронных данных в уголовных делах органов общественной безопасности КНР от 15.05.2019[484] и уведомлению ВНП КНР 2021 г., допускается криминалистическая экспертиза электронных данных (кит. «电子数据取证主要»): сбор и извлечение электронных данных (кит. «收集、提取电子数据»), электронная проверка данных и эксперименты по расследованию (кит. «电子数据检查和侦查实验»), идентификация данных (кит. «电子数据检验与鉴定»).

Первое подразумевает собой изъятие и опломбирование оригинальных носителей информации (кит. «扣押、封存原始存储介质»); извлечение электронных данных на месте (кит. «现场提取电子数据») или из сети «Интернет» (кит. «网络在线提取电子数据»); консервация или замораживание электронных данных (кит. «冻结电子数据»); поиск электронных данных (кит. «调取电子数据»); резервное копирование данных (кит. «制作、封存电子数据备份»); видеозапись производимых следственных действий (кит. «对收集、提取电子数据的相关活动进行录像»). В сравнении с иными рассмотренными юрисдикциями последнее действие очевидно выделяется и обеспечивает подлинность и достоверность полученных доказательств.

В случае передачи аудиовизуальных материалов и электронных данных, собранных с помощью технических средств, копия должна быть сделана двумя или более следователями, с указанием такой информации как местоположение оригинальных доказательств и оригинального носителя информации, и подписана лицом, создающим её, и с прикрепленной печатью подразделения.

---

[484] 公安机关办理刑事案件电子数据取证规则 [Правила сбора электронных данных для органов общественной безопасности для рассмотрения уголовных дел] // Бюро общественной безопасности Чунцина. URL: https://gaj.cq.gov.cn/zslm_245/wlaqgl/flfg/201912/t20191221_2043591.html (дата обращения: 20.03.2025).

Хотя предпочтительнее использовать уже известные механизмы получения или сохранения электронных данных, опытный следователь (прокурор) может воспользоваться экспериментальными передовыми методиками, однако они должны не нарушать фундаментальные права человека и быть обоснованными. Только в этом случае они могут быть приняты. При этом методология должна быть воспроизводимой, чтобы другое должностное лицо могло восстановить последовательность действий. Механизм должен вызывать доверие и обеспечивать сохранность и отслеживаемость доказательств[485].

Фактически в большинстве актов (Исполнительных правилах к Закону АРЕ № 175-2018, Мнениях КНР 2022 г. и уведомлении ВНП КНР 2021 г., Постановлении Главы судебной власти ИРИ) подразумевается документирование электронных доказательств с указанием времени, даты, компетентного лица с его подписью, операционной системы и её версии, наименованием используемых программ и команд, содержания сведений, оборудования, ПО и устройства.

В индонезийской юридической литературе предлагается вести так называемую цепочку хранения с указанием деталей собранных доказательств, личностей всех сторон, ответственных за доказательства, продолжительности хранения доказательств, любой передачи доказательств (включая подписи участвующих сторон)[486]. Фактически это возможно реализовать через ЭДО и Блокчейн.

Ввиду технической составляющей деяний **место преступления** может пониматься двойственно: физическое (традиционный компонент) и цифровое пространство (виртуальный компонент). Что касается первого, то обратимся к Мнениям КНР 2022 г.: под местом совершения преступления понимается места расположения серверов онлайн-сервисов, используемых для осуществления преступной деятельности, местоположение поставщиков сетевых услуг,

---

[485] Geschonneck A. Computer-Forensik. Computerstraftaten erkennen, ermitteln, aufklären. 5. aktualisierte und erweiterte Auflage. Heidelberg: dpunkt Verlag, 2011. S. 66 и Ахмад Хамао, Ала Аваад, Вала Абдулла. Электронные доказательства (юридические и технические аспекты). Палестина: Юридический институт Бирзейтского университета, 2015. С. 19 (на араб. яз.).
[486] Bara Pratama Mahaputra, Chairul Muriman, Surya Nita. Указ. Соч.

местонахождение нарушенных информационных сетевых систем и их менеджеров, а равно информационных сетевых систем, которые использовались подозреваемыми, обвиняемыми или потерпевшими, места, где потерпевшим нанесен вред или где имели место потери имущества. В Руководстве Арабского университета наук безопасности им. принца Наифа бин Абдель Азиза 2024 г. используется термин «цифровое место преступления» (араб. «مسح الجريمة الرقمي»), указывая на содержание электронных устройств (электронные файлы и их метаданные, журналы и системные записи) и внешних носителей информации, их характеристики и идентификаторы в адресном пространстве (IP- и MAC-адреса), а также криминалистически значимую информацию, находящуюся в ИТС (учётные записи социальных сетей, аккаунты электронных почтовых ящиков и облачные хранилища).

В качестве одной из современных особенностей расследования киберпреступлений отметим нарастающее использование ИИ (или как минимум широкое обсуждение этого вопроса)[487]. Например, при выявлении экстремистских взглядов в социальных сетях[488]. В ноябре 2020 г. Центр ИИ и робототехники Исследовательского института УНП ООН совместно с Министерством внутренних дел ОАЭ запустили инициативу «ИИ для более безопасных детей» (англ. «Artificial Intelligence for Safer Children») для разработки инструмента по эффективному мониторингу и выявлению запрещённого контента, а также жертв торговли людьми среди несовершеннолетних. В июле 2022 г. была издана онлайн-платформа, которая активно используется не только сотрудниками Департамента по защите детей МВД ОАЭ, но и правоохранительными органами других стран Глобального Юга[489]. Определённую пользу могут составить и отдельные нейронные сети для анализа

[487] Шестак В.А., Цыплакова А.Д. Проблемы совершенствования прогнозирования преступности // Расследование преступлений: проблемы и пути их решения. 2023. № 3 (41). С. 78–84.
[488] Ajala I., Shanaz F., El Barachi M., Oroumchian F., Sujith M., Rand Y., Lutfi S. Combining artificial intelligence and expert content analysis to explore radical views on twitter: case study on far-right discourse // Journal of Cleaner Production. 2022. № 362. 132263.
[489] AI for Safer Children // UNICRI. URL: https://unicri.org/topics/AI-for-Safer-Children (accessed 12.04.2025).

больших массивов информации, в том числе мониторинга социальных сетей[490]. С учётом расширенной дорожной карты Федеральной публичной прокуратуры ОАЭ 2045 г. и заключённого соглашения с компанией «AI71» внедряются технологии по 3D-симуляции мест происшествия [491], электронному документообороту на основании Блокчейна и искусственного интеллекта в целях отслеживания изъятых предметов, хранения конфиденциальной информации, обеспечения цепочки хранения и, как следствие, сохранности цифровых доказательств[492].

§ 2. Наложение ограничительных и иных мер по исполнению антиотмывочного законодательства в отдельных странах Глобального Юга

При рассмотрении т.н. антиотмывочного законодательства в отдельных странах Глобального Юга необходимо для начала определиться с **понятийным аппаратом** и его содержанием.

В Федеральном декрете-законе ОАЭ № 20 от 2018 г. «О противодействии отмыванию денег и борьбе с финансированием терроризма и деятельности незаконных организаций» (далее — ФДЗ ОАЭ № 20-2018)[493] под *аль-амвалю* (араб. «الاموال») понимаются активы, независимо от способа их приобретения, вида и формы, материальные или нематериальные, движимые или недвижимые, электронные, цифровые или зашифрованные, включая национальную валюту, иностранную валюту, а также юридические документы и акты, независимо от их

---

[490] Barakat W. How Dubai Police use AI to act on 'alarming' social media posts, protect children online // Khaleej Times. 12.11.2024. URL: https://www.khaleejtimes.com/business/tech/how-dubai-police-use-ai-to-act-on-alarming-social-media-posts-protect-children-online (accessed 12.05.2025).

[491] В отечественной юридической мысли подобное обозначается как киберполигоны. См. Хатов Э.Б. Киберполигон как платформа цифровых компетенций следователей криминалистов // Советская и российская криминалистика: традиции и перспективы: Материалы всероссийской научно-практической конференции с международным участием, Москва, 02 февраля 2023 года. Москва: Московская академия Следственного комитета Российской Федерации, 2023. С. 210-213.

[492] Dajani H. UAE to speed up criminal case processing by 100% using AI, blockchain // Khaleej Times. 05.05.2025. URL: https://www.khaleejtimes.com/uae/uae-speed-up-criminal-cases-ai-blockchain (accessed 12.05.2025).

[493] مرسوم بقانون اتحادي في شأن مواجهة جرائم غسل الأموال ومكافحة تمويل الإرهاب وتمويل التنظيمات غير المشروعة [Федеральный Декрет-закон ОАЭ № 20 от 2018 г. «О противодействии отмыванию денег и борьбе с финансированием терроризма и деятельности незаконных организаций»] // Законодательная база ОАЭ. URL: https://www.uaelegislation.gov.ae/en/legislations/1016?keyword=laundering (дата обращения: 08.04.2025).

формы, включая электронную или цифровую форму, которые доказывают право собственности на эти активы, акции или права, связанные с ними, а также экономические ресурсы, которые считаются активами любого рода, включая природные ресурсы, а также банковские кредиты, чеки, платежные поручения, акции, ценные бумаги, облигации, векселя, аккредитивы, а также любые проценты, прибыль или другие доходы, полученные или возникающие в результате этих активов, и они могут использоваться для получения любого финансирования, товаров или услуг. Данная дефиниция совпадает с подходом КСА: согласно Положению КСА от 03.10.2012 «О борьбе с террористическими преступлениями и его финансированием»[494], *аль-амвалю* включает в себя электронные или цифровые системы, банковские кредиты, которые обозначают право собственности или долю в них, а также все виды коммерческих и финансовых ценных бумаг или любые другие проценты, прибыль или доход, полученные от таких средств.

В Законе АРЕ № 80 от 2002 г. «О борьбе с отмыванием денег» (далее — Закон АРЕ № 80-2002)[495] используются термины «активы» (араб. «الاصول») или «деньги» (араб. «الاموال») как синонимы, согласно поправкам (Законы № 36 от 2014 г. и № 17 от 2020 г.), и даются примеры экономических ресурсов — нефть и иные природные ресурсы. В указе короля Бахрейна № 4 от 31.01.2001 «Об издании закона о запрещении и борьбе с отмыванием денег и финансировании терроризма»[496] (в ред. от 01.10.2020) данный список дополняется произведениями искусства, антиквариатом, ювелирными изделиями и драгоценными металлами, а также товарными знаками и правами интеллектуальной собственности.

---

[494] نظام مكافحة جرائم الإرهاب وتمويله [Положение о борьбе с террористическими преступлениями и его финансированием] // Бюро экспертов Совета министров Королевства Саудовская Аравия. URL: https://laws.boe.gov.sa/BoeLaws/Laws/LawDetails/57694209-3eed-46c7-a5d8-a9ed012761d4/1 (дата обращения: 08.04.2025).

[495] قانون رقم ٨٠ لسنة٢٠٠٢ بإصدار قانون مكافحة غسل الأموال المعدل بالقانون رقم ٧٨ لسنة ٢٠٠٣ [Закон № 80 от 2002 года о принятии Закона о борьбе с отмыванием денег с поправками, внесенными Законом № 78 от 2003 года] // Центральный банк Арабской Республики Египет. URL: https://www.cbe.org.eg/-/media/project/cbe/page-content/rich-text/laws-and-regulations/laws/ar/antimoneylaunderinglaw-ar-other-laws-2.pdf (дата обращения: 08.04.2025).

[496] مرسوم بقانون رقم ٤ لسنة ٢٠٠١ بشأن حظر ومكافحة غسل الاموال وتمويل الارهاب [Указ коорля Бахрейн № 4 от 2001 г. «Об издании закона о запрещении и борьбе с отмыванием денег и финансировании терроризма»] // Комиссия по законодательству и правовому мнению Королевства Бахрейн. URL: https://www.lloc.gov.bh/FullAr/L0401.docx (дата обращения: 08.04.2025).

Сходным образом обозначается и интерпретируется термин в иранском законодательстве — *мал* (перс. «مال») — это любой тип активов, будь то материальные или нематериальные, движимые или недвижимые, законные или незаконные, и любой тип финансовой выгоды или привилегии, а также все документы, подтверждающие права, как на бумажных носителях, так и в электронном виде, такие как коммерческие документы, акции или ценные бумаги (п. «ب» ст. 1 Закона ИРИ от 22.01.2008, в ред. от 03.08.2018 «О борьбе с отмыванием денег»[497]).

Отдельного внимания заслуживает рассмотрение активов, имеющих выражение в виртуальном пространстве, поскольку выявлено множество используемой терминологии.

В марте 2020 г. Департаментом надздора и контроля национальной платежной системы ЦБ ИХК было проведено подробное исследование[498]. Самым широким термином является цифровая валюта (араб. «العملة الرقمية»), включающая в себя электронные, легальные цифровые, то есть выпущенные центральными банками (араб. «الرسمية»), виртуальные (араб. «الإفتراضية»), в том числе зашифрованные (крипто) валюты (араб. «العملات المشفرة»), не имеющие физического присутствия, торгующие и обращающиеся через сеть Интернет.

У виртуальных валют нет единой правовой базы, центрального надзорного органа и легального обеспечения. Они делится на два вида: открытая или конвертируемая (араб. «القابلة للتحويل») в легальную валюту, которая делится на централизованную и децентрализованную; неконвертируемая или закрытая конвертируемая (араб. «القابلة غير للتحويل»). Примером первой категории виртуальной валюты является Биткоин (децентрализованная) и электронное/цифровое золото (англ. «e-gold») (централизованная).

---

[497] قانون مبارزه با پولشویی [Закон о борьбе с отмыванием денег] // Законодательная база ИРИ. URL: https://davoudabadi.ir/page/1896240/قانون-مبارزه-با-پولشویی (дата обращения: 08.04.2025).

[498] В случае расхождений позиций, мнение авторов (сотрудников ЦБ) является независимым. См. подробнее العملات المشفرة [Зашифрованные валюты] // Central Bank of Jordan. URL: https://www.cbj.gov.jo/EchoBusV3.0/SystemAssets/8f23f11e-de4c-4538-91f7-82aab2d7bf04.pdf (дата обращения: 08.04.2025).

Стейблкоины (араб. «العملات الرقمية الثابتة أو المستقرة») рассматриваются и как разновидность цифровой валюты, и как тип криптовалюты. При этом сама криптовалюта может обозначаться и как виртуальная валюта, и как зашифрованный актив (араб. «الأصول المشفرة»). Под зашифрованным активом понимается хранимый цифровый актив, основанный на технологии распределенного реестра, а также зашифрованное цифровое представление стоимости или договорных прав, которые основаны на технологии распределенного реестра и могут быть переданы, сохранены или обменены в электронном виде. К ним относятся криптовалюты и два вида токенов (араб. «رموز»): утилитарные (араб. «الخدمات») и ценная бумага (араб. «الأوراق المالية»). Однако отметим, что, например, согласно поправкам 2023 г. к Модулю 6 «Криптоактивы» Руководства Центрального банка Королевства Бахрейн [499] правовой статус любых цифровых токенов определён как ценные бумаги.

Ввиду того что криптовалюты не обладают функциями расчетной единицы, средства сбережения и платежа, наиболее точным термином для обозначения биткоина и других «криптовалют» является «зашифрованный актив» или «криптоактив». Центральный банк ИРИ 28.01.2019 подготовил «Требования и правила в сфере криптовалют». В нём указывается, что под криптовалютой (фарси «ارز رمزچایه») понимается финансовый актив на цифровой платформе блокчейна. 27.02.2022 правительство ИРИ выпустило документ «Трансформация национального правительства», в котором криптовалюта определяется как финансовый актив, содержащий стоимость, которую можно обменять на рынках капитала, или как платежный инструмент[500].

Под электронными деньгами (араб. «النقود الإلكترونية») понимается преобразование в нетрадиционную форму денежной стоимости в конкретной валюте, выпущенной в виде электронных данных, хранящихся в компьютерных

[499] Crypto-Asset Module. Rulebook of the Central Bank of Bahrain // Central Bank of Bahrain. URL: https://cbben.thomsonreuters.com/sites/default/files/net_file_store/Vol_6_CRA_2023.pdf (accessed 08.04.2025).

[500] Ghamami S.M.M., Alipoor M. A comparative study of exposure to cryptocurrencies in the Iranian and American legal systems // Encyclopedia of Economic Law Journal. 2022. № 29(21). P. 150-184 (in Persian).

сетях, однако на практике возникает путаница в терминологии, что прослеживается в законодательстве арабских стран и фатвах.

Понятие виртуальных активов (дословно с араб. «الأصول الافتراضية» виртуальные источники) было дано в поправках к ФДЗ ОАЭ № 20-2018 в 2021 г. Под ними понимается цифровое представление стоимости, которой можно торговать или которую можно передавать в цифровой форме, а также использовать для платежных или инвестиционных целей и т.д. в соответствии с тем, что указано в Исполнительном регламенте. Фактически данное определение перекликается с той дефиницией, что дана в Руководстве ФАТФ[501]. В решении Совета министров ОАЭ № 111 от 12.12.2022 «Об организации виртуальных активов и поставщиков виртуальных услуг»[502] уточняется, что под это понятие не попадает цифровое представление фиатных валют, ценных бумаг и других *аль-амвалю* — независимо от способа их приобретения, вида и формы, материальные или нематериальные, движимые или недвижимые, электронные, цифровые или зашифрованные, включая национальную валюту, иностранную валюту, а также юридические документы и акты, независимо от их формы, включая электронную или цифровую форму, которые доказывают право собственности на эти активы, акции или права, связанные с ними, а также экономические ресурсы.

Согласно Закону Эмирата Дубай № 4 от 28.02.2022 «О регулировании виртуальных активов в Эмирате Дубай»[503], к рассматриваемой категории также относят виртуальные токены — цифровое представление прав, предлагаемые и

---

[501] Руководство по применению риск-ориентированного подхода. Виртуальные активы и провайдеры услуг виртуальных активов // ФАТФ. URL: https://www.fatf-gafi.org/content/dam/fatf-gafi/translations/guidance/MUMCFM-FATF-Guidance-RBA-VA-VASPs.pdf (дата обращения: 08.04.2025).

[502] قرار مجلس الوزراء رقم (111) لسنة 2022 بشأن تنظيم الأصول الافتراضية ومزودي خدماتها [Решение Совета министров ОАЭ № 111 от 12.12.2022 «Об организации виртуальных активов и поставщиков виртуальных услуг»] // Онлайн база Совета министров ОАЭ. URL: https://laws.uaecabinet.ae/ar/materials/law/1623 (дата обращения: 08.04.2025).

[503] Law No. 4 of 2022 on Regulating Virtual Assets in the Emirate of Dubai // The Dubai Virtual Assets Regulatory Authority. URL: https://rulebooks.vara.ae/sites/default/files/en_net_file_store/VARA_EN_338_VER1.pdf (accessed 08.04.2025).

находящиеся в обороте на платформе виртуальных активов (поставщика виртуальных услуг).

В Решении председателя Совета директоров Управления по ценным бумагам и товарам ОАЭ № 21/R.M от 11.01.2020 «О регулировании криптоактивов»[504] используется термин «криптоактивы» (араб. «الأصول المشفرة»), под которым понимается запись в электронной сети или базе данных распространения, которые действуют как средство обмена, средство сбережения, расчетная единица, представление собственности, имущественных прав или прав доступа, а равно выгоды любого рода, которая может быть передана в электронном виде от одного лица к другому посредством работы компьютерной программы или алгоритма, регулирующих её использование.

Аль-амвалю / *мал* или активы следует ограничивать от двух терминов:

- средства или *васаауту* (араб. «وسائط») или инструменты (англ. «instrumentality», амхар. «የወንጀል መፈጸሚያ») — то, что является или предназначено для использования каким-либо образом при совершении преступления или правонарушения;

- *мутахасоляятун* (араб. «متحصلات»), *ävайед* (перс. «عواید حاصل از جرم»)[505], доходы (англ. «proceeds of crime»), плод преступления (амхар. «የወንጀል ፍሬ») — денежные средства или активы, прямо или косвенно возникающие или полученные от совершения любого запрещённого законом деяния (действия или бездействия) или правонарушения[506], включая прибыль, привилегии, экономические выгоды и любые аналогичные средства, полностью или частично переведенные в другие активы. При этом *ävайед* понимается шире и охватывает не только «результат преступления», но и предмет, а также средства или орудия совершения деяния.

---

[504] قرار رئيس مجلس إدارة الهيئة رقم ٢٣ لسنة ٢٠٢٠ م بشأن النظام الخاص بأنشطة الأصول المشفرة [Решение Председателя Совета директоров Управления № 23 от 2020 года о системе деятельности с криптоактивами] // Управление по ценным бумагам и товарам ОАЭ. URL: https://www.sca.gov.ae/Content/Userfiles/Assets/Documents/f79fbf6.pdf (дата обращения: 08.04.2025).

[505] Взаимозаменяемо с *мал* (перс. «مال حاصل از جرم»).

[506] Не во всех случаях предусмотрено второе. Например, в ИКХ речь только про преступления.

В ФДРЭ, Республиках Индия и Индонезия более лаконичные подходы к определению активов / имущества (англ. «funds» / «property», индонез. «Harta Kekayaan»): недвижимость и недвижимость, материальные и нематериальные (телесные и нетелесные) объекты, включая различные документы и права на них. Более того, в Законе Республики Индия № 15 от 17.01.2003 «Об отмывании денег» указывается, что для данных целей во избежание сомнений имущества любого рода, используемое для совершения отмывания денег или предикатных преступлений. Столь изящная оговорка избавляет от сомнений, попадают ли виртуальные активы в данное понятие и могут ли на них налагаться ограничительные меры.

В КНР реализована несколько иная конструкция: вместо легального определения активов, указываются источники и способы отмывания денег и финансирования терроризма что в общеуголовном законе, что в Законе КНР «Об отмывании денег в Китайской Народной Республике», принятом 31.10.2006, пересмотренном 08.11.2024 и вступившем в силу с 01.01.2025[507], а также в совместном объяснении Верховной Народной Прокуратуры КНР и Верховного Суда КНР от 19.08.2024[508]. В качестве таковых признаётся незаконный оборот наркотиков, организованная преступность, террористические преступления, контрабанда, коррупция и взяточничество, деяния, подрывающие порядок финансового управления, финансовое мошенничество, операции с виртуальными активами, методы обмена финансовыми активами, азартные игры, смешивание с операционным доходом денежных ресурсоемких мест, фиктивные операции, ложные требования и долги, ложные гарантии, ложная отчётность о доходах,

---

[507] 中华人民共和国反洗钱法 [Закон о борьбе с отмыванием денег Китайской Народной Республики] // Правительство КНР: официальный сайт. URL: https://www.gov.cn/yaowen/liebiao/202411/content_6985765.htm (дата обращения: 21.04.2025).

[508] 最高人民法院 最高人民检察院 关于办理洗钱刑事案件适用法律若干问题的解释 发布时间: 2024 年 8 月 19 日 [Объяснение нескольких вопросов применимого законодательства при уголовных делах об отмывании денег Верховным Судом и Верховной Народной Прокуратурой от 19.08.2024] // Верховная Народная Прокуратура КНР: официальный сайт. URL: https://www.spp.gov.cn/xwfbh/wsfbt/202408/t20240819_663652.shtml#2 (дата обращения: 21.04.2025).

операции с лотерейными билетами, предоплаченными картами, золотом и другими драгоценными металлами и иные.

В то время как законодательством материкового Китая запрещены транзакции с криптовалютой, в одном из САР (Гонконг) разработан подробный закон, содержащий определения виртуальных активов (англ. «virtual assets», кит. «虛擬資產») и внутриигровых активов (англ. «in-game assets», кит. «遊戲用資產»). Первое несколько шире, чем то, что содержится в Глоссарии ФАТФ, охватывая две группы: криптографически защищенное цифровое представление стоимости, обладающее нижеперечисленными признаками, либо цифровое представление стоимости, указанное в качестве виртуального актива в уведомлении, опубликованном в установленном порядке Комиссией в официальной газете.

К характеристикам первого относят четыре признака:

- выражение как расчётной единицы или средства сбережения экономической стоимости;

- использование или предназначение в качестве средства обмена, приемлемого для общественности, для одной или нескольких целей (оплата товаров или услуг; погашение долга, инвестиции);

- предоставление прав, правомочий или доступа к голосованию по управлению, администрированию или руководству делами, связанными с любым изменением условий любого соглашения, применимого к любому криптографически защищенному цифровому представлению стоимости;

- возможность передачи, хранения или продажи в электронном виде; соответствие требованиям Комиссии.

Внутриигровой актив обозначает любое цифровое представление ценности, которое куплено или иным образом приобретено человеком, не выражено в какой-либо валюте, выдаётся как часть игры и может быть использовано лицом только для оплаты или обмена на виртуальные объекты или виртуальные услуги в игре, использоваться лицом для оплаты или обмена на любые аналогичные вещи в игре или в связи с ней или использоваться лицом для оплаты или обмена на любую аналогичную вещь, являющуюся частью игры. При этом он не включается в

понятие виртуальных активов, поскольку относится к ограниченным цифровым токенам (кит. «有限用途數碼代幣») (те в свою очередь исключены из перечня виртуальных активов)[509].

Ограничительные меры включают в себя *арест* (араб. «الحجز», англ. «*arrest*»), *замораживание* (араб. «التجميد», англ. «*freezing*», амхар. «ማገድ»), *конфискацию* (араб. «المصادرة», англ. «*confiscation*», перс. «ضبط», амхар. «መውረስ») активов, полученных преступным путём. В Индии выделяется также общий термин «*attachment*» — запрет передачи, преобразования, распоряжения или перемещения имущества по приказу. В то время как *арест или замораживание* предполагают временный запрет на перевод, перемещение, изменение или распоряжение *активами* любым способом на основании приказа/распоряжения компетентного органа, конфискация — безвозвратное лишение частных *активов*, доходов или средств, которые используются или предназначены для использования каким-либо образом для совершения тяжкого преступления или правонарушения в соответствии с решением компетентного суда. Предметом ареста выступают инструменты (араб. «المعدات»), средства и имущество, в то время как замораживание возможно в отношении денежных средств и приравненных к ним объектов.

Примечательно, что, несмотря на подробность (в различной степени) регламентации понятийного аппарата в отдельных странах Глобального Юга, отсутствуют нормы, узконаправленные на изъятие и хранение именно виртуальных и иных активов, имеющих выражение в виртуальном мире. Исходя из логики построения законов, применим общий порядок, а технические вопросы оставляются на усмотрение конкретных специалистов.

Нормативно-правовой базой выступает не только уголовно-процессуальное, но и антиотмывочное, и антикоррупционное законодательство. Последнее характерно в особенности для Республики Индонезия. Помимо общего

---

[509] «2022 年打擊洗錢及恐怖分子資金籌集(修訂)條例草案» [Законопроект о борьбе с отмыванием денег и финансированием терроризма (поправка) 2022 г.] // Законодательный совет Специального административного района Гонконг. URL: https://www.legco.gov.hk/tc/legco-business/council/bills.html?bill_key=10015&session=2022 (дата обращения: 06.06.2025).

регулирования, выделяется также специальное в рамках СФЗ и САР. Не для всех государств характерна конфискация без обвинительного приговора, в частности для Индии, что подтверждается судебной практикой Верховного суда РИ[510]. Например, в Совете народных представителей Республики Индонезия рассматривается законопроект о возврате преступных активов, где предусмотрена конфискация без обвинительного приговора в случае, если лицо не может объяснить происхождение активов с распространением концепции на членов семьи, родственников и лиц, причастных к организованной преступности[511].

Общий механизм получения данных о подозрительных трансакциях или деятельности, нарушающей закон, происходит обычно через ПФР, а наложение ограничительных мер выглядит следующим образом: судебный (Республика Индонезия, ФДРЭ, КСА, ТР), внесудебный (Республика Индия, Катар) и смешанный (ОАЭ, Бахрейн, АРЕ) подходы.

Обычно в Центральном банке[512] или в качестве независимого органа создано независимое подразделение финансовой информации (ПФР), в которое отправляются отчеты о подозрительных операциях и связанная с ними информация от всех финансовых учреждений, деловых нефинансовых предприятий и профессий, а также поставщиков услуг по виртуальным активам, работает над их изучением и анализом и направляет их в компетентные органы автоматически или по запросу. Оно может направить запрос финансовым учреждениям, деловым и

---

[510]Vijay Madanlal Choudhary and Others v. Union of India and Ors. (2022 SCC Online SC 929) // Supreme Court of Republic of India. URL: https://scr.sci.gov.in/scrsearch/?p=pdf_search/home&text=Vijay%20Madanlal%20Choudhary&captcha=md7fMd&search_opt=PHRASE&fcourt_type=undefined&escr_flag=&proximity=&sel_lang=&neu_cit_year=&neu_no=&ncn=&citation_vol=&citation_yr=&citation_supl=&citation_page=&app_token= (accessed 02.06.2025).

[511] Khalila A. Rejuvenasi KPK: Urgensi Pemberlakuan Rancangan Undang-Undang Perampasan Aset dengan Pendekatan In Rem dan Tinjauan Pendekatan Serupa pada Regulasi Unexplained Wealth di Australia [Обновление КПК: срочность принятия проекта закона о конфискации активов с подходом In Rem и рассмотрение аналогичного подхода к регулированию необъясненного богатства в Австралии] // Институт научных исследований Юридического факультета Университета Индонезии. URL: https://lk2fhui.law.ui.ac.id/portfolio/rejuvenasi-kpk-urgensi-pemberlakuan-rancangan-undang-undang-perampasan-aset-dengan-pendekatan-in-rem-dan-tinjauan-pendekatan-serupa-pada-regulasi-unexplained-wealth-di-australia/ (дата обращения: 02.06.2025).

[512] Характерно для арабских стран.

нефинансовым предприятиям и профессиям, поставщикам услуг по виртуальным активам и заинтересованным сторонам предоставить любую дополнительную информацию или документы, связанные с полученными ими отчетами и информацией, а также другую информацию, которую они считают необходимой для выполнения своих задач, в срок и в формате, указанных подразделением.

При расследовании и сборе выводов по предикатному преступлению правоохранительные органы учитывают степень, в которой финансовые аспекты, связанные с преступной деятельностью, связаны с преступлением отмывания денег, финансирования терроризма или финансированием незаконных организаций, с целью определения масштабов преступления, выявления и отслеживания *аль-амвалю* и любых других средств, которые могут подлежать конфискации, и доказательств преступления.

Прокуратура может изучить мнение ПФР по полученным ею отчетам о случаях отмывания денег, финансирования терроризма и финансирования незаконных организаций.

Что касается внесудебного механизма с возможностью обжалования в судебном порядке, то Глава ЦБ арабских государств или его заместитель могут распорядиться о замораживании *аль-амвалу*, подозреваемых финансовыми учреждениями, на определённый законом срок, в соответствии с правилами и средствами контроля, и срок может быть продлен Генеральным прокурором или его уполномоченным представителем. В ИХК срок не превышает 5 рабочих дней; в ОАЭ — 7 рабочих дней; в Катаре — 10 дней. В АРЕ не указан срок замораживания, однако предусмотрен срок для подачи ходатайства о подтверждении запрета распоряжаться средствами в суд — 7 дней.

Наиболее подробно процедура регламентирована в эмиратском регулировании. Государственное обвинение и компетентный суд ОАЭ[513] могут, в зависимости от обстоятельств, распорядиться об идентификации, отслеживании или оценке *аль-амвалю,* доходов и подозрительных средств или их эквивалентной

[513] В то время как в ИХК и АРЕ схоже, в КСА и ТР — только суд.

стоимости, изъятых или замороженных, если они получены в результате преступления или связаны с ним, без предварительного уведомления их владельца и распорядиться о запрете на поездки до конца расследования или судебного разбирательства. В зависимости от дела и при необходимости принимать решения, которые препятствуют торговле или распоряжению *аль-амвалю*, поступлениями и средствами, указанные органы принимают необходимые меры для предотвращения любого поведения, направленного на уклонение от изданных распоряжений о замораживании или изъятии без ущерба для прав добросовестных третьих лиц. При этом решения о замораживании средств в финансовых учреждениях, лицензированных Центральным банком, осуществляются только через него.

Жалоба на приказ прокуратуры о конфискации или замораживании должна быть передана в компетентный суд. Если жалоба отклонена, то новая не может быть подана до истечения трех месяцев с даты отклонения первой, если только не возникнет серьезная причина подавать до истечения этого срока. Жалоба должна быть подана с отчетом в компетентный суд, и председатель суда определяет слушание, о котором он должен сообщить истцу, а прокуратура представляет меморандум о своем заключении по жалобе, и суд принимает решение по нему в течение периода, не превышающего 14 рабочих дней с даты ее подачи.

В зависимости от обстоятельств эмиратские государственное обвинение и компетентный суд поручают тому, кого они сочтут целесообразным, управлять *аль-амвалу,* доходами и средствами, изъятыми или которые были заморожены или подлежат конфискации, и санкционировать их реализацию или продажу на публичных торгах даже до вынесения решения, если это необходимо. Например, в случаях, если их стоимость снизится с течением времени либо предмету может быть нанесен ущерб. Доход от их реализации или продажи поступает в Государственное казначейство в случае окончательного осуждения.

В Египте же распоряжение о наложении временных ограничительных мер может выноситься Генеральным прокурором или Главным военным прокурором по просьбе председателя Совета попечителей подразделения по борьбе с отмыванием денег и финансированием терроризма; арест имущества подозреваемого, его

супруги/супруга и несовершеннолетних детей — уголовными судами или Генеральным прокурором (п. «ا» ст. 208.2 Закона АРЕ № 150 от 1950 года «Об уголовных мерах» (в ред. Закона № 189 от 05.09.2020) [514]). В Бахрейне арест накладывается исполнительным органом (араб. «للوحدة المنفذة»), назначенным министром внутренних дел, с уведомлением прокуратуры в трехдневный срок и возможностью обжаловать в судебном порядке (в течение 15 дней).

Отметим, что в Законе ИРИ от 22.01.2008 «О борьбе с отмыванием денег» (в ред. от 03.08.2018) не предусмотрено точной процедуры наложения ограничительных мер, однако судебная практика указывает на превалирование именно судебного подхода[515].

В рамках **международного сотрудничества в сфере уголовного судопроизводства** (далее — МССУС) наложение ограничительных мер осуществляется при направлении запросов об оказании взаимной правовой помощи по уголовным делам[516], которые исполняются уполномоченным[517] органом через судебный механизм. При этом запросы по отмыванию денег, финансированию терроризма и предикатным деяниям, например, в ОАЭ считаются высокоприоритетными.

В Республике Индонезия возможно задействование двух направлений МССУС при необходимости наложении ограничительных мер:

---

[514] قانون الإجراءات الجنائية رقم 150 لسنة 1950 [Закон АРЕ № 150 от 1950 года «Об уголовных мерах»] // Законодательная база АРЕ. URL: https://manshurat.org/node/14676 (дата обращения: 06.05.2025).

[515] Цыплакова А. Д. Противодействие криптовалютным преступлениям в странах Среднего и Ближнего Востока и Северной Африки // Противодействие криптовалютным преступлениям в зарубежных странах. М.: ООО Издательский дом «Юрлитинформ», 2025. С. 402-490.

[516] В арабоязычной юридической литературе арест и конфискация активов и доходов, полученных преступным путем (араб. «ضبط ومصادرة متحصلات وعائدات الجرائم») признаётся самостоятельной формой МССУС. См. подробнее محمد محمود الكمالي. أحكام التعاون القضائي الدولي في المسائل الجنائية في دولة الإمارات العربية المتحدة [Мухаммад Махмуд Аль-Камали. Положение о международном судебном сотрудничестве по уголовным делам в Объединенных Арабских Эмиратах] // Журнал судебных исследований Министерства юстиции ОАЭ. № 3. URL: https://elaws.moj.gov.ae/Adel.aspx?val=UAE-FokehAA1 (дата обращения: 18.12.2024).

[517] В Бахрейне, например, подобный орган назначается по решению МВД. В ОАЭ и АРЕ разрешается вопрос через общие положения ВПП по УД, соответственно, компетентным органом выступает Министерство юстиции; в КСА — Постоянно действующий комитет по запросам правовой помощи.

- запросы о взаимной правовой помощи по уголовным делам включают помощь на этапах исполнения окончательных судебных решений, отслеживания, замораживания, конфискации и ареста активов, полученных преступным путём — что является классическим подходом;

- запросы о выдаче лиц могут сопровождаться просьбами о конфискации активов, согласно Закону Республики Индонезия № 1 от 18.01.1979 «О выдаче»[518] — более нетривиальный, но исторически давно известный способ.

Согласно ст. ст. 43–45 Закона Республики Индонезия № 9 от 2013 г. «О предупреждении и искоренении уголовного преступления финансирования терроризма» [519] иностранное государство или иностранная юрисдикция могут направить правительству Индонезии запрос о помощи в проведении блокирования средств, предположительно находящихся в Индонезии или расположенных в ней, принадлежащих лицу или корпорации, чья личность указана в списке подозреваемых террористов и террористических организаций, составленном иностранным государством или иностранной юрисдикцией, на основе национальных внешнеполитических интересов, международных договоров или добрых отношений, основанных на принципе взаимности.

С точки зрения правового основания могут выступать национальное регулирование, универсальные и региональные конвенции, двусторонние межгосударственные или межправительственные соглашения и принцип взаимности. При этом круг применимых международно-правовых документов разнится:

- ЛАГ: Эр-Риядское соглашение о судебном сотрудничестве, Арабская конвенция против транснациональной организованной преступности (Каир,

---

[518] Undang-undang (UU) Nomor 1 Tahun 1979 tentang Ekstradisi [Закон Республики Индонезия от 18.01.1979 «О выдаче»] // Законодательная база Республики Индонезия. URL: https://peraturan.bpk.go.id/Details/47145/uu-no-1-tahun-1979 (дата обращения: 09.02.2025).

[519] Pencegahan dan Pemberantasan Tindak Pidana Pendanaan Terorisme [О предупреждении и искоренении уголовного преступления финансирования терроризма] // Законодательная база Республики Индонезия. URL: https://peraturan.bpk.go.id/Details/38846/uu-no-9-tahun-2013 (дата обращения: 09.02.2025).

21.12.2010), Арабская конвенция по борьбе с коррупцией (Каир, 21.12.2020)[520], Арабская конвенция по борьбе с отмыванием денег и финансированием терроризма (Каир, 21.12.2010), Соглашение об исполнении судебных решений 1952 г.;

- ССАГПЗ: Соглашение об исполнении судебных решений, представлений и заявлений в странах ССАГПЗ;

- АС: Конвенция о предупреждении терроризма и борьбе с ним (Аддис-Абеба, 01.07.1999), Конвенция о предупреждении коррупции и борьбе с ней (Мапуту, 11.07.2003);

- Совет Европы: Конвенция об уголовной ответственности за коррупцию (Марокко присоединилась, но не ратифицировала);

- IGAD: Конвенция Межправительственного органа по развитию об экстрадиции и Конвенция Межправительственного органа по развитию о взаимной правовой помощи по уголовным делам (не вступили в силу, однако ФДРЭ подписала и ратифицировала);

- АСЕАН: Договор о взаимной правовой помощи по уголовным делам (Куала-Лумпур, 29.11.2004);

- Содружества Наций (применимо к Республике Индия): Харарская схема взаимной правовой помощи по уголовным делам, Конвенции Ассоциации регионального сотрудничества Южной Азии об оказании взаимной правовой помощи по уголовным делам.

Межгосударственное взаимодействие в ИРИ регулируется на сегодняшний день только двусторонними соглашениями об оказании взаимной правовой помощи по уголовным делам в отсутствие всеобъемлющего закона о судебном сотрудничестве. Принцип же взаимности может именоваться специфически. Так, например, согласно постановлению Министра юстиции и прав человека Республики Индонезия № 12 от 08.07.2022 «О взаимной помощи в уголовных вопросах в рамках Министерства права и прав человека» [521] он обозначается как

---

[520] Тунис не ратифицировал её.

[521] Penanganan Bantuan Timbal Balik dalam Masalah Pidana di Lingkungan Kementerian Hukum dan Hak Asasi Manusia [Обработка взаимной помощи по уголовным вопросам в Министерстве права и прав человека] // Законодательная база Республики Индонезия. URL:

добрые отношения [522] (индонез. «atas dasar hubungan baik berdasarkan prinsip resiprositas») при наличии соответствующего письменного обязательства: «Pemerintah [nama Negara Peminta] menyatakan keseenggupannya nahna di masa yang akan dating akan memberikan beentuan kepada Pemerintah Indonesia untuk bantuan yang serupa dalam masalah pidana» / «*Правительство [наименование запрашивающей страны] заявляет о своей готовности оказать содействие правительству Индонезии в будущем в аналогичной помощи по уголовным делам*».

Необходимо учитывать, что в зависимости от процедуры, направления МССУС и применимых оснований центральные органы могут разниться (обычно Министерства юстиции или внутренних дел, а также Генеральная прокуратура). Например, в заявлении КНР к Конвенции ООН против коррупции (Мерида, 31.10.2003) указывается, что центральным органом по оказанию взаимной помощи выступает Верховная народная прокуратура, в то время как в заявлении КНР к Конвенции против транснациональной организованной преступности (Нью-Йорк, 15.11.2000) от 29.03.2006 назначены Министерство юстиции и Министерство общественной безопасности.

В Республике Индонезия центральным органом по оказанию взаимной правовой помощи по уголовным делам выступает Министерство юстиции и по правам человека, однако непосредственным исполнителем при соблюдении судебного механизма выступает Генеральная прокуратура, которая в свою очередь подаёт ходатайство в суд о выдаче постановления на арест активов в местный окружной суд, и при условии удовлетворения ходатайства исполняет его в соответствии с действующим уголовно-процессуальным законом и объявляет об

---

https://peraturan.bpk.go.id/Details/225563/permenkumham-no-12-tahun-2022 (дата обращения: 09.02.2025).

[522] В пояснительной записке (индонез. «PENJELASAN») к Закону Республики Индонезия № 1 от 03.03.2006 «О взаимной правовой помощи по уголовным делам» под добрыми отношениями понимаются дружественные отношения, руководствующиеся национальными интересами и основанные на принципах равенства, взаимной выгоды и соблюдения как национальных, так и международных законов. См. подробнее Undang-undang (UU) Nomor 1 Tahun 2006 tentang Bantuan Timbal Balik dalam Masalah Pidana [Закон Республики Индонезия № 1 от 03.03.2006 «О взаимной правовой помощи по уголовным делам»] // Законодательная база Республики Индонезия. URL: https://peraturan.bpk.go.id/Details/40151/uu-no-1-tahun-2006 (дата обращения: 09.02.2025).

изъятии не менее чем в двух национальных ежедневных газетах. Министерство юстиции и по правам человека Республики Индонезия уведомляет запрашивающее государство о ходе исполнения запроса и организует передачу изъятого имущества.

Компетентным органом в отношении запросов блокирования средств при финансировании терроризма выступает начальник Национальной полиции Индонезии, который подаёт ходатайство в окружной суд Центральной Джакарты для принятия решения. При удовлетворении такового начальник Национальной полиции Индонезии направляет определение о блокировании поставщику финансовых услуг (индонез. «Pengguna Jasa Keuangan») или в уполномоченное учреждение, которые должны немедленно заблокировать средства лиц, включенных в список подозреваемых террористов и террористических организаций, по запросу иностранного государства или иностранной юрисдикции.

Основанием для отклонения запроса не могут являться следующие случаи:

1) преступление включает в себя финансовые, налоговые[523] или таможенные вопросы;

2) обязательные положения о конфиденциальности для финансовых учреждений и конкретных нефинансовых предприятий и профессий, которые не нарушают действующее в стране законодательство, если только соответствующая информация не была получена в обстоятельствах, в которых применяются юридические профессиональные привилегии или профессиональная тайна;

3) преступление является политическим или связанным с ним;

4) связь запроса с преступлением, которое является предметом расследования или судебного разбирательства, проводимого в государстве, если только запрос не помешает расследованиям или разбирательствам в стране;

5) тот факт, что деяние, на котором основан запрос, не является преступлением в государстве или не имеет общих черт преступления, предусмотренного в нём;

---

[523] Аналогично в Республике Индия банковская тайна не является основанием для отказа.

6) тот факт, что преступное деяние в государстве указано под другим названием или описанием или что его элементы в запрашиваемом государстве различаются.

Любопытно, что в Законе АРЕ № 80-2002 указан более узкий перечень, включены лишь обязательные положения о конфиденциальности финансовых учреждений, налоговых вопросов при непротиворечении основным принципам правовой системы страны.

Зачастую в отдельных странах Глобального Юга предусматривается процедура обжалования и учёт интересов третьих лиц (добросовестных владельцев или бенефициаров). Отметим проблематику отсутствия единого механизма возврата преступных активов [524], что характерно не только для России, но и изучаемых государств.

§ 3. Применение процессуальных мер по исполнению информационного законодательства в отдельных странах Глобального Юга

Исполнение информационного регулирования и применения отдельных мер в государствах Глобального Юга невозможно без рассмотрения цифровизации уголовного судопроизводства и смежных областей, в частности касающихся введения электронного документооборота и использования видеоконференцсвязи. В части процессуальных мер отметим меры процессуального принуждения, ограничения доступа к неправомерному или запрещённому контенту и Интернет-ресурсам, а также трансграничную передачу данных.

Постановлением Главы судебной власти ИРИ от 24.05.2016 «Правила использования компьютерных и телекоммуникационных систем» [525], принятого во

---

[524] Старжинская А. Н. Современный подход к расследованию в отношении активов, полученных в результате совершения преступлений // Уголовный процесс и криминалистика: правовые основы, теория, практика, дидактика (к 75-летию со дня рождения профессора Б. Я. Гаврилова): сборник научных статей по материалам международной научно-практической конференции, Академия управления МВД России, 03 ноября 2023 года. Москва: Академия управления МВД России, 2023. С. 391-396.

[525] آیین نامه نحوه استفاده از سامانه های رایانه ای یا مخابراتی [Правила использования компьютерных и телекоммуникационных систем] // Официальная база законодательства ИРИ. URL: https://rc.majlis.ir/fa/law/show/984023 (дата обращения: 12.04.2025).

исполнение раздела 9 Уголовно-процессуального закона ИРИ от 03.07.2013, предусмотрено создание следующих систем в рамках Национальной сети правосудия под руководством Национального центра данных судебной системы при Центре судебной статистики и информационных технологий ИРИ: системы управления судебными делами (перс. «سامانه مدیریت پرونده قضایی»; «سمپ» — САМП); системы электронных судебных услуг (перс. «سامانه خدمات الکترونیک قضایی», «سخا» — САКХА), системы электронных уведомлений (перс. «سامانه ابلاغ») и иные, необходимые для создания учётных записей, с целью подачи сообщений о преступлении, ходатайств, жалоб, исков, вызова лиц, вручения судебных документов, уведомлений, получения приказов и распоряжений, направления результатов действий, обжалования и исполнения решений. Судебные органы и должностные лица обязаны использовать эти системы в процессах расследования и исполнения приговоров.

Электронная форма или содержание судебных документов и бумаг, уведомлений, направлений дел, повесток обвиняемых, судебного представительства, публикации объявлений, подписей и отпечатков пальцев, сертификатов соответствия оригиналу, финансовых операций, адресов являются достаточными и действительными и на всех стадиях расследования и принудительного исполнения (будь то гражданского или уголовного). Невозможно отказать в подтверждении их юридической силы и правовых последствий исключительно на основании формы или способа обмена электронной информацией.

Если будут созданы и предоставлены необходимые возможности, то электронные меры заменят неэлектронные. Параллельные действия в невиртуальном пространстве запрещены.

Система уведомлений действует для сторон обвинения и защиты (спора), их законных представителей, экспертов, должностных лиц и судебных органов. Уведомлением считается электронное поступление судебных документов в личный кабинет пользователя-получателя в соответствующей системе. Их видимость сохраняется с указанием времени и других данных, и к ней приписываются все

последствия фактического уведомления в документарном виде. Вход в систему уведомлений через свою учётную запись и просмотр документов с её помощью является подтверждением получения. При электронном уведомлении адресат может ссылаться на неосведомлённость, если докажет, что он не был проинформирован о содержании уведомления из-за отсутствия доступа или неисправностей в компьютерной или телекоммуникационной системе. Отказ от обращения в систему уведомления считается отказом в принятии судебных документов.

Если адресат содержится в следственном изоляторе, тюрьме или исправительном учреждении, то уведомление будет отправлено на учетную запись пользователя тюрьмы, следственного изолятора или этих учреждений в дополнение к учётной записи пользователя-адресата. Вышеуказанные органы будут нести ответственность за реализацию уведомления в соответствии с регламентом и обязаны направлять результаты уведомления документов в судебный орган через систему уведомления. Если у получателя нет учётной записи пользователя, то органы обязаны создать для него учётную запись и предоставить получателю доступ к системе оповещения, соблюдая при этом принципы безопасности.

В Республике Индонезия допускается судопроизводство по уголовным делам и производство отдельных процессуальных действий в электронной форме с 2018 г.[526] (регулирования Верховного суда Республики Индонезия № 3 от 2018 г., № 1 от 2019 г., № 4 от 2020 г. в ред. регулирования ВС РИ № 8 от 2022 г.). Как проведение судебных заседаний (особенно в период пандемии COVID-19), так и допрос свидетелей производились в формате видеоконференцсвязи[527]. Второе имело место при допросе лиц из иностранных государств (ФРГ, Сингапура и Малайзии) по нескольким делам ввиду необходимости получения сведений (раскрытия истины со ссылкой на решение ВС РИ № 354/Пид.Б/2002/ПН), но невозможности их

[526] А Конституционным судом РИ была реализована данная идея ещё в 2009 г.

[527] Zulaeha M. E-Courts in Indonesia: Exploring the Opportunities and Challenges for Justice and Advancement to Judicial Efficiency // International Journal of Criminal Justice Sciences. 2023. № 18 (2). P. 183–194, Saputro H.D., Fatoni S. Persidangan Perkara Pidana Secara Elektronik Dalam Sistem Peradilan Pidana Di Indonesia Di Masa Pandemi Covid-19 // INICIO LEGIS. 2022. № 3 (2). P. 142–161.

физического присутствия. По решению ВС РИ № 12/ПК/Пид/2006 было допрошено лицо на территории консульства РИ в ФРГ по коррупционному делу (растрата небюджетных средств), поскольку оно сопровождало супругу на лечение и не могло присутствовать в зале суда. По решению ВС РИ № 008/КМА/СК/И/2011 в ходе судебного заседания по делу о террористических актах на Бали были допрошены семь лиц на территориях посольств РИ в Сингапуре и Малайзии по ходатайству прокуратуры, при этом только один из свидетелей не был допрошен в ходе предварительного расследования [528] . Отметим, что при этом в уголовно-процессуальном законодательстве РИ подобного не предусмотрено[529]. Однако в решениях ВС отмечалось следующее: использование ИТ позволяет преодолеть возникающие препятствия для отправления правосудия, достичь материальной истины и эффективности, отвечая обязательству судей установить применимые нормы (индонез. «rechtsvinding», англ. «finding law») и допуская соблюдение всех формальностей по типу принесения присяги. Данные случаи рассматриваются как проявление *lex spesialis* в индонезийской юридической литературе[530].

В рассматриваемых странах Ближнего и Среднего Востока использование систем видеоконференцсвязи и других электронных систем связи для допроса сторон, получения показаний свидетелей или заключений экспертов предусмотрено напрямую либо уголовно-процессуальным регулированием (e.g., АНДР[531], КСА), либо же киберзаконодательством (например, ОАЭ), охватывая не только уголовное судопроизводство, но и предоставление иных государственных услуг в рамках одной или нескольких систем. Примером служит платформа

---

[528] Pemberian Keterangan Saksi Lewat Videoconference Dalam Rancangan KUHAP. Jakarta: Institute for Criminal Justice Reform, 2015. P. 3–4.

[529] Nashriana N.A.A., Isma Nurillah I. Persidangan Perkara Pidana Di Pengadilan Secara Elektronik Pada Masa Pandemi Covid-19 Ditinjau Dari Asas Peradilan Pidana // Simbur Cahaya. 2021. № 28 (1).

[530] Barlian A.A.E., Latipulhayat A., Rusmiati E., Wulandari W., Sukma A.N.A. Electronic Criminal Justice in Indonesia: Challenges and the Future Measures // Jambura Law Review. 2025. № 1(7). P. 243–274.

[531] Отметим, что в АНДР не по всем видам преступлений, а только при рассмотрении дел о коррупции, деяниях террористической направленности и организованной преступности. См. подробнее Yaghla M., Kenaza S. Digitization of litigation procedures in Algeria: between consolidating the modernization of justice and violating the fundamental principles of litigation // Russian Law Journal. 2025. Vol. 1. P. 1141–1156.

«Наджиз» в КСА (араб. «ناجز»)[532]. Более того, в отдельных прокуратурах (например, эмирата Дубай) внедрены умные системы по ведению уголовного дела с адаптацией к различным правовым системам мира, реорганизацией и структурированию информации[533], получения разрешения на проведение обысков, вызову сторон и направлению уведомлений, изданию приказов о блокировке незаконного контента с использованием технологий Блокчейн на основании безбумажной стратегии Дубай с 2021 г. и расширенной дорожной карты Федеральной публичной прокуратуры ОАЭ 2045 г.[534]. Однако в ряде государств (в частности, в Алжире) есть технические и организационные препятствия для внедрения цифровых проектов ввиду разного уровня развития ИТ.

В сфере международного сотрудничества уголовного судопроизводства и международного полицейского сотрудничества допускается использование электронных форм для обмена информацией и направления запросов о взаимной правовой помощи по уголовным делам (ст. 16 Закона АНДР № 04-09, Руководящие принципы международного судебного сотрудничества по уголовным делам ОАЭ от 2021 г.[535], Руководство Постояннодействующего комитета по запросам правовой помощи КСА по правовой помощи и процедурам возврата активов [536]). С

---

[532] إبراهيم محمد شاكر علي، مشعل بن أحمد الشريده. تسخير التكنولوجيا لخدمة القانون والقضاء والأفراد التقاضي الإلكترونيُّ ومنصة ناجز في المملكة العربيَّة السعوديَّة أنموذجًا [Ибрагим Мохаммед Шакер Али, Мешаль бин Ахмед Аш-Шарида. Использование технологий в интересах закона, судебной системы и частных лиц Электронный судебный процесс и платформа Najeez в Королевстве Саудовская Аравия в качестве модели] // Ассоциация юристов АРЕ. 09.11.2023. URL: https://egyls.com/تسخير-التكنولوجيا-لخدمة-القانون-والق/ (дата обращения: 02.05.2025).

[533] Создание аннотаций к изображениям, аудиозаписям и видеоклипам, их расшифровка, извлечение информации и правовых принципов и их мгновенная привязка к тематическим фактам, прецедентам, а также представление юридических мнений, способствующих всестороннему упрощению судебных процессов.

[534] UAE's Criminal Case Processing to Be Enhanced With AI & Blockchain // Scene Now UAE. 06.05.2025. URL: https://cairoscene.com/buzz/uae-s-criminal-case-processing-to-be-enhanced-with-ai-blockchain (accessed 02.06.2025), Public Prosecution develops AI-supported work system // WAM. 17.10.2024. URL: https://www.wam.ae/en/article/b5q8wqe-public-prosecution-develops-ai-supported-work (accessed 02.06.2025).

[535] الدليل الإسترشادي للتعاون القضائي الدولي في المسائل الجنائية [Руководящие принципы международного судебного сотрудничества по уголовным делам] // Министерство юстиции ОАЭ. URL: https://www.moj.gov.ae/Content/Userfiles/Assets/Documents/8e8f1221.pdf (дата обращения: 08.04.2025).

[536] دليل إجراءات المساعدة القانونية واسترداد الموجودات [Руководство по правовой помощи и процедурам возврата активов] // Министерство внутренних дел Королевства Саудовская Аравия. URL:

Департаментом международного сотрудничества, исполнения судебных решений и ухода за заключенными Генеральной прокуратуры Египта можно связаться по электронной почте для координации, неофициальных консультаций или изучения возможных исключений.

Цифровизация коснулась и избирательной системы на различных уровнях, и органов (исполнительные и законодательные / совещательные), включая удалённую регистрацию и голосование. В 2022 г. в Омане МВД разработало и внедрило приложение «Интихаб» (с араб. «إِنْتِخَابٌ» — избрание) совместно с Министерством информационных технологий и коммуникаций СО, полицией, Маджлисом Аш-шура СО и соответствующими институтами; в 2023 г. модернизовало и внедрило ИИ для озвучивания слепым и разъяснения глухим порядка реализации активного избирательного права, добавились платформы «Сафхатун» (с араб. «صَفْحَةٌ» — лицо) и «Хиваарун» (с араб. «حِوَارٌ» — ответ) для общения с кандидатами и разрешения возможных проблем[537]. С юридической точки зрения нарушения, связанные с перечисленными системами и приложениями, относятся к посягательствам на либо АСОД, либо веб-сайты, либо приложения.

С точки зрения **мер процессуального принуждения** при совершении киберпреступлений отметим электронный контроль или мониторинг[538], запрет пользоваться любой информационной сетью, системой или ИТ оборудованием, а равно помещение в лечебный приют или реабилитационный центр как по судебному постановлению, так и по решению Генерального прокурора (ст. 59 ФДЗ ОАЭ № 34-2021).

Что касается **ограничения доступа** к неправомерному контенту и Интернет-ресурсам, то отметим несколько особенностей регулирования стран Глобального Юга: различия в подходах определения незаконного (сомнительного) контента (наряду с расплывчатостью формулировок), широта либо узконаправленные случаи

---

https://www.moi.gov.sa/wps/wcm/connect/dc92bbae-005f-497d-9829-5d8e26d6135f/200.pdf?MOD=AJPERES&CVID=mvFff1Y (дата обращения: 08.04.2025).

[537] Lasledj N., Bouzoualeg Kh. Electronic elections in Algeria: between reality and expectations comparative study with the Omani experience // Russian Law Journal. 2025. № 13 (1). P. 447–456.

[538] При этом в АНДР электронный мониторинг является следственным действием.

применения норм, административный и смешанный порядки реализации данного института.

Согласно ст. 62 ФДЗ ОАЭ № 34-2021, во время расследования деяний против государственной безопасности компетентные органы могут по собственной инициативе или по просьбе Генерального прокурора ОАЭ издать приказ о корректировке/исправлении, удалении, закрытии и запрете доступа (блокировке) в связи с публикацией, переизданием или распространением неправомерного контента или контента, содержащего ложные данные, и направить его, в том числе в электронном виде. Под деяниями против государственной безопасности в данном случае понимаются:

- преступления, предусмотренные указанным ФДЗ ОАЭ № 34-2021 и совершенные в интересах или от имени иностранного государства, террористической группы, банды, организации или незаконного органа;

- проникновение в информационные системы государственных учреждений (ГУ) или их повреждение, повреждение информационных систем общественно важного объекта, подлог электронной почты, электронных сайтов и электронных учётных записей ГУ, незаконные перехват и раскрытие сообщения, информации или данных ГУ;

- сбор и обработка конфиденциальных данных и информации в нарушение законодательства, публикация данных или информации, которые не соответствуют стандартам медиаконтента;

- призыв к нарушениям положений Конституции и законов, их пропаганда, подстрекательство к несоблюдению законодательства, одобрение и пропаганда терроризма, распространение информации, которая наносит ущерб интересам государства;

- подстрекательство к нанесению ущерба государственной безопасности и нападению на должностных лиц уголовного судопроизводства, содействие подстрекательству к мятежу и нанесению вреда национальному единству;

- осквернение и ущерб репутации государства и государственной символики, оскорбление иностранного государства;

- призывы к проведению демонстраций без разрешений и их пропаганда;

- проведение статистических исследований или опросов без лицензии с умыслом на оказание влияния или нанесения ущерба интересам государства;

- распространение слухов и ложных новостей, предоставление незаконного контента и отказ от его удаления, а равно получение дара для совершения указанной деятельности.

Что касается стандартов медиаконтента, то обратимся к регулированию арабоязычных стран, в частности к ст. 17 Федерального декрета-закона ОАЭ № 55 от 02.10.2023 «О регулировании медиа»[539], ст. 28 Исполнительного регламента указанного ФДЗ (Постановление Совета министров ОАЭ № 68 от 10.06.2024)[540], Приложению 2 Постановления Совета министров ОАЭ № 42 от 16.04.2025 «О регулировании административных правонарушений и наказаний, связанных с регулированием деятельности средств массовой информации», Положению КСА от 13.12.2017 «Об аудио-визуальных СМИ» (указ короля КСА № M/33)[541] и ст. 37 Закона № 88.33 от 10.08.2016 «О прессе и издательском деле» (Дахир №1.16.122)[542], сгруппировав их следующим образом:

- *уважение* к Богу, исламу, Священному Корану, Пророку Мухаммаду, его женам и последователям, монотеистическим религиям и другим верованиям и неоскорбление ни одного из них; системе правления в государстве, её символов и институтов, а также высших интересов государства и общества, ориентации и политики государства на внутреннем и международном уровне; правилам

---

[539] مرسوم بقانون اتحادي في شأن تنظيم الإعلام [Федеральный декрет-закон «О регулировании медиа»] // Законодательная база ОАЭ. URL: https://uaelegislation.gov.ae/ar/legislations/2145 (дата обращения: 02.05.2025).

[540] قرار مجلس الوزراء في شأن اللائحة التنفيذية للمرسوم بقانون اتحادي في شأن تنظيم الإعلام [Постановление Совета министров «Исполнительный регламент к Федеральному декрету-закону о регулировании медиа»] // Законодательная база ОАЭ. URL: https://uaelegislation.gov.ae/ar/legislations/2547 (дата обращения: 02.05.2025).

[541] نظام الإعلام المرئي والمسموع [Положение «Об аудио-визуальных СМИ»] // Бюро экспертов Совета министров КСА. URL: https://laws.boe.gov.sa/BoeLaws/Laws/LawDetails/ed5fdbc0-c183-4a8a-a8b7-a9ed004b5900/1 (дата обращения 02.05.2025).

[542] القانون رقم ٨٨.١٣ المتعلق بالصحافة والنشر الصادر بظهير شريف رقم ١.١٦.١٢٢ صادر في ٦ ذي القعدة ١٩٣٧ (١٠) أغسطس ٢٠١٦ // الجريدة الرسمية. ٢٠١٦. ١١. ٥٩٦٦-٥٩٨٧ ص. [Закон № 88.13 «О прессе и издательском деле», изданный Королевским указом № 1.16.122 от 6 зуль-кида 1937 (10) августа 2016 г. // Официальный вестник. 2016. № 11. С. 5966-5987.]

неприкосновенности частной жизни и всё, что связано с частной жизнью человека; культурному и цивилизационному наследию и национальной идентичности государства; культуре, самобытности и ценностям государства;

- *не подвергать* воздействию что-либо, что может навредить внешним сношениям государства[543];

- *не публиковать и не распространять что-либо*, что оскорбляет национальное единство и социальную сплочённость; может подстрекать к совершению преступлений[544];

- *не публиковать, не передавать и не распространять* ложные новости, поддельные документы или неверно приписанные юридическим и физическим лицам; информацию, которая может нанести ущерб национальной валюте или экономической ситуации в стране; фразы, изображения, рисунки или мнения, нарушающие святость общественной морали, оскорбляющие молодежь, призывающие к принятию или продвижению деструктивных идей — общественные интересы, порядок и безопасность; порнографические или непристойные материалы, в том числе подстрекающие к проституции, домогательству или сексуальному насилию в отношении несовершеннолетних;

- *публиковать* сведения о ходе дел по клевете, личном статусе, особенно касающиеся доказательства отцовства и развода (без разрешения суда); судебных документов по делам несовершеннолетних или в отношении совершеннолетних, позволяющие установить личность детей;

- *не разжигать* межконфессиональную, региональную и племенную рознь, не подстрекать к насилию, ненависти и террористическим актам, не разжигать

---

[543] Отметим разницу эмиратского и саудовского регулирования. В указанном Положении КСА указаны арабские, исламские и дружественные страны. В Марокко указывается на запрет оскорбления личности или достоинства глав государств, правительств, министров иностранных дел, иностранных дипломатических или консульских представителей, аккредитованных или делегированных Его Величеству Королю.

[544] В эмиратских стандартах, среди прочего, указывается «поощрять убийства, изнасилования, употребление наркотических средств и психотропных веществ», в то время как в саудовских — пропаганда наркотиков, табака, алкоголя, а в Марокко — подстрекательство к убийству, посягательствам на физическую неприкосновенность человека, терроризму, краже или саботажу, а равно восхвалять военные преступления, преступления против человечности, геноцид или терроризм.

ненависть и не сеять раздор в обществе[545], не подстрекать к причинению вреда несовершеннолетним;

- *не оскорблять* ценности, преобладающие в обществе, и учитывать требования общественных интересов, правовую, экономическую, судебную систему и систему безопасности в стране;

- *не распространять* слухи и недостоверные новости;

- *не пропагандировать* идеи групп по политическим, этническим, экономическим, идеологическим, мировоззренческим или социальным признакам, деструктивно настроенным против государства и служащим своим собственным интересам;

- *выбирать* правильных лиц [546] при размещении или принятии их выступлений в СМИ;

- *соблюдать* возрастную классификацию художественных произведений, утверждённую компетентным органом, и права ребёнка в соответствии с действующим в стране законодательством[547].

Отдельно выделим сочетание принципов свободы выражения мнений и контроль со стороны государства, особенно в части оговорки о «*lèse majesté*», содержащейся как в общеуголовных законах (e.g., Бахрейн), так и в специальных актах (КСА).

В ОАЭ одно из наиболее подробных регулирований с точки зрения регламентации процедуры среди арабских государств: в течение 3 рабочих дней с даты уведомления об издании приказа на него может быть подана жалоба. В течение недели после получения жалобы компетентный орган должен принять решение; оставление без ответа по истечении срока рассматривается как отклонение. Данное решение может быть обжаловано в судебном порядке с предоставлением

---

[545] В КСА в качестве угрозы рассматривается подстрекательство к терроризму и действиям, угрожающим как национальному, так и международному миру, провокация раскола, ненависти, насилию.

[546] В ОАЭ указывается на моральные качества личности, в КСА — единообразный скромный внешний вид, пристойную одежду, отсутствие наготы, вульгарной лексики.

[547] В решениях Верховного совета по регулированию СМИ АРЕ 2022–2024 гг. отражена схожая концепция.

доказательств и документов в течение недели с даты принятия решения по жалобе — в федеральный суд, расположенный в столице Федерации (ОАЭ). Суд рассматривает апелляцию в совещательной палате и принимает решение по ней в течение семи дней. Он может отменить приказы полностью или частично либо отклонить апелляцию после рассмотрения ходатайств ответчиков. Решение суда является окончательным.

Закрытие веб-сайта полностью или частично навсегда или на определённый срок возможно и по решению суда в случае осуждения лица за киберпреступление по ФДЗ ОАЭ № 34-2021.

В Эфиопии же нет закона, который регулировал бы сомнительный контент (англ. «problematic content») в Интернете, в том числе порядок блокировки, фильтрации или удаления противоправного, оскорбительного и наносящего вред контента. Если правительство считает, что определённый контент является сомнительным, оно обычно даёт указание единственному государственному оператору связи — компании «Ethio-telecom» — заблокировать доступ к контенту или вообще весь веб-сайт.

Исходя из системного толкования ряда актов, в частности Прокламаций ФДРЭ № 1284 от 18.04.2023 «Об эфиопской цифровой идентификации» [548], № 1185 от 23.03.2020 «О предупреждении и пресечении разжигании ненависти и дезинформации» [549], № 759 от 27.08.2012 «О рекламе» [550], отметим подробную регламентацию стандартов рекламирования и расплывчатость формулировок иного контента. По общему правилу реклама не должна противоречить закону или морали, содержать вводящих в заблуждение или несправедливых заявлений, уважать социальные и традиционные ценности общества, уважать профессиональный кодекс этики, защищать интересы и достоинство государства. К первой категории относят нарушения достоинства, свободы или равенства в отношении языка, пола,

---

[548] Proclamation No. 1284/2023 Ethiopian Digital Identification Proclamation // Federal Negarat Gazette. 2023. № 19. P. 14715.

[549] Proclamation No. 1185/2020 Hate Speech and Disinformation Prevention and Suppression Proclamation // Federal Negarat Gazette. 2020. № 26. P. 12339.

[550] Proclamation No.759/2012 Advertisement Proclamation // Federal Negarat Gazette. 2012. № 59. P. 6520.

расы, нации, национальности, профессии, религии, убеждений, политического или социального статуса, правил хорошего поведения или человеческого достоинства отдельных лиц, нации, народностей или народов, а также порочение репутации организации; подрыв национальных или региональных государственных флага, герба, гимна или валюты, унижение достоинства или эмоционального состояния человека с физическими недостатками[551] или ВИЧ/СПИДом, а равно страдающего от другого заболевания; провокация хаоса, насилия, террора, конфликта или страха; подстрекательство к действиям, которые могут поставить под угрозу физическое или психическое здоровье и безопасность людей; звуковое загрязнение выше установленных государством нормативов; непристойные представления; нарушение прав интеллектуальной собственности и использование изображений лица без его/её согласия; противоречие безопасности движения или охране окружающей среды; использование знаков отличия и формы сил обороны или полиции; содержание или форма подачи запрещены другими законами или способствуют нарушению какого-либо закона. Ко второй — ложная информация, ущемление интересов покупателей, смешивание иностранного языка с местным, двусмысленность, безосновательное использование превосходной степени и иные.

Запрещаются также высказывания, которые намеренно поощряют ненависть, дискриминацию или нападки на человека либо различимую группу лиц по признакам этнической принадлежности, религии, расы, пола или физических ограничений, а равно являются ложными и распространяются лицом, которое знало или должно было знать о ложности информации, и с высокой вероятностью может вызвать общественные беспорядки, бунт, насилие или конфликт.

Как отмечают учёные[552], проводились комплексные исследования для Министерства связи и информационных технологий Эфиопии и ожидалась

---

[551] Любопытно, что ограничения по здоровью и различные заболевания по-разному указываются в подобных нормах. Например, в Законе Республики Индонезия № 11 от 02.01.2024 «О внесении изменений в Закон № 11 2008 г. об электронной информации и транзакциях» (далее — Закон РИ № 11-2024), помимо физических недостатков, также указываются умственные. При этом выделение ВИЧ/СПИД в Прокламации ФДРЭ № 1185/2020 тоже является нетипичным.

[552] Yilma K.M. Указ. Соч.

разработка способов классификации и удаления сомнительного контента. Тем не менее до сих пор подобного не принято.

Регулирование в рассматриваемой сфере в ряде государств Глобального Юга находится на начальной стадии развития и зачастую остаётся на усмотрение компетентных органов или регулируется подзаконными актами. Схожая ситуация в плане размытости стандартов медиаконтента наблюдается, например, в Индонезии и Катаре. Только в начале 2025 г. в Катаре началось обсуждение подобного[553].

Тем не менее не во всех азиатских государствах можно выделить такую тенденцию. Согласно Информационно-технологическим правилам РИ, посредники в (значимых) социальных сетях и онлайн-играх обязаны проявлять должную осмотрительность (англ. «due diligence») в отношении сведений, которые:

- принадлежат другому лицу, на которое пользователь не имеет никаких прав;

- носят непристойный, порнографический, педофилический характер или нарушают неприкосновенность частной жизни другого лица, включая личную жизнь, оскорбляют или преследуют по признаку пола, расы или этноса, касаются отмывания денег, азартных игр или онлайн-игр, причиняющих вред пользователю, или поощряют их; пропагандирует вражду между различными группами по признаку религии или касты с целью подстрекательства к насилию;

- наносят вред ребенку;

- нарушают патент, торговую марку, авторское право или другие права интеллектуальной собственности;

- содержат обман или вводят в заблуждение адресата относительно происхождения сообщения или сознательно и намеренно передают любую дезинформацию или информацию, которая является явно ложной и неправдивой или вводящей в заблуждение по своей природе, а равно в отношении любого предприятия Центрального правительства, идентифицируется как фальшивая, ложная или вводящая в заблуждение компетентным подразделением Центрального

---

[553] Qatar's New Legal Framework for Regulating Digital Content Creation // Mashael Al Sulaiti Law Firm. 12.01.2025. URL: https://www.mas.com.qa/news/qatars-new-legal-framework-for-regulating-digital-content-creation (accessed 02.05.2025).

правительства по проверке фактов, которое Министерство может указать в уведомлении, опубликованном в Официальном вестнике;

- посредством которых лицо выдаёт себя за другое лицо;

- угрожают единству, целостности, обороне, безопасности или суверенитету Индии, дружественным отношениям с иностранными государствами или общественному порядку, или подстрекает к совершению любого наказуемого преступления, или препятствует расследованию любого деяния, или оскорбляет другую нацию;

- содержит программный вирус или любой другой компьютерный код, файл или программу, предназначенные для прерывания, уничтожения или ограничения функциональности любого компьютерного ресурса;

- имеют характер онлайн-игры, которая не подтверждена как допустимая;

- имеют характер рекламы или суррогатной рекламы или продвижения онлайн-игры, которая не является допустимой онлайн-игрой, или любого посредника в онлайн-играх, предлагающего такую онлайн-игру;

- нарушают любой действующий закон.

Предусмотрена внесудебная процедура по ограничению и блокировке неправомерного контента, то есть посягающего на интересы суверенитета и целостности Индии, безопасность государства, дружественные отношения с иностранными государствами, общественный порядок, приличия или мораль, в связи с неуважением к суду, диффамацией, подстрекательством к преступлению, с возможностью судебного надзора (раздел 69А Закона РИ № 21-2000).

Ранее директор Национального центра кибербезопасности был должностным лицом, назначаемым для целей принятия решений об ограничении или блокировке контента (англ. «designated officer»). Ныне Центральное правительство в лице Министерства электроники и информационных технологий Республики Индия посредством публикации уведомления в Официальной газете назначает компетентных лиц. На апрель 2025 г. избраны главы, секретари и учёные различных

категорий из 64 ведомств в качестве координаторов (англ. «nodal officers»), а также отдельные лица из штатов (35)[554].

Получив запрос от министерства, департамента правительства Индии или штата, назначаемое лицо направляет уведомление лицу/субъекту, контролирующего веб-сайт, и указывает время и дату для направления ответа и уточнений. Рассмотрением запроса занимается специальный комитет. По его заключению Секретарю Департамента ИТ Министерства электроники и информационных технологий Республики Индия направляется рекомендация. При удовлетворении такового назначаемое должностное лицо поручает управлению или посреднику исполнить приказ об ограничении или блокировке. В случаях, не терпящих отлагательств, оно может сразу напрямую направить свои доводы Секретарю Департамента ИТ, который в письменном виде фиксирует причины блокировки или издаёт решение как промежуточную меру без заслушивания сторон. В течение 48 часов комитет должен принять решение об удовлетворении или отклонении запроса. Отметим, что определение срочности (англ. «emergency») остаётся в дискреции компетентных должностных лиц.

В случае с Карти П. Чидамбарам против Бюро иммиграции (дело № 874 от 2018 г.), Достопочтенный Высокий суд Мадраса постановил, что любое решение, будь то исполнительное или квази-судебное, подлежит судебному пересмотру в соответствии со ст. 226 Конституции Индии от 26.11.1949. Потерпевшее лицо может потребовать от Суда поручить правительству предоставить причины для блокировки веб-сайта и отменить запретительные приказы по существу или за несоблюдение естественной справедливости (дело Анурадха Бхасин).

---

[554] List of Nodal Officers from States of India under the provisions of Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009 // Ministry of Electronics and Information Technology, Government of India. URL: https://www.meity.gov.in/static/uploads/2024/12/ec8bee89ce950acd9ad5920c074146e7.pdf (accessed 02.05.2025); List of Nodal Officers from Ministries/Departments of Central Government under the provisions of Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009 // Ministry of Electronics and Information Technology, Government of India. URL: https://www.meity.gov.in/static/uploads/2024/12/b67f3564f0dc9df27f5eed565b600ce8.pdf (accessed 02.05.2025).

Сложившаяся практика свидетельствует об отзывах или отменах приказов как в рамках судебных разбирательств, так и при проведении дополнительных слушаний, включая возможность принять корректирующие меры, если это сочтёт необходимым, хотя такой механизм и не был предусмотрен в соответствии с Правилами блокировки ИТ (уведомление от 27.10.2009[555]). Примерами могут служить дела Высокого суда Дейли: Танул Тхакур против Союза Индии и Орс. от 11.05.2022[556] и Ракиб Хамид против Союза Индии, представленного секретарем Министерства электроники и информационных технологий и Анр. от 25.04.2024[557].

Закон РИ № 11-2024 содержит расплывчатые формулировки в отношении незаконного контента — нарушающий положение законов и нормативных актов (индонез. «melanggar ketentuan peraturan perundang-undangan»), моральные принципы (индонез. «kesusilaan»), общественный порядок (индонез. «ketertiban umum»), содержащий угрозы насилия или запугивания, а также ложная информация, вызывающая беспорядки в обществе, представляющий опасность для жизни и здоровья отдельных лиц или общества. При этом правительство имеет право прекратить доступ или издать приказ организаторам электронных систем (индонез. «Penyelenggara Sistem Elektronik») прекратить доступ к информации или документам, имеющим противоправное содержание, а равно видоизменить их (ст. 40 Закона РИ № 11-2024). Согласно пояснениям к Постановлению Правительства Республики Индонезия № 71 от 10.10.2019 «О внедрении электронных систем и транзакций»)[558] к нарушению положений законов и иных нормативных правовых

---

[555] Notification. New Delhi, 27.10.2009 // India Code: Digital Repository of Laws. URL: https://upload.indiacode.nic.in/showfile?actid=AC_CEN_45_76_00001_200021_1517807324077&type=rule&filename=blocking_for_access_of_information_rule_2009.pdf (accessed 02.05.2025).

[556] Tanul Thakur vs. Union of India & Ors., W.P.(C) 13037/2019 // Delhi High Court. URL: https://dhcappl.nic.in/dhcorderportal/GetOrder.do?ID=mmh/2022/1669727751905_9807_2022.pdf (accessed 02.05.2025).

[557] Raqib Hameed vs. Union of India represented by the Secretary Ministry of Electronics and Information Technology & Anr., W.P.(C) 5820/2024 // Delhi High Court. URL: https://dhcappl.nic.in/dhcorderportal/GetOrder.do?ID=smp/2024/724909941714372150536_96365_58202024.pdf (accessed 02.05.2025).

[558] Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik [Правительственное постановление номер 71 2019 года о внедрении электронных систем и транзакций] // Министерство телекоммуникаций и информатики Республики Индонезия. URL:

актов относят электронную информацию и/или электронные документы, которые содержат элементы порнографии, азартных игр, клеветы и/или диффамации, мошенничества, ненависти к племенам, религиям, расам и межгруппам (англ. «SARA»), насилие и/или жестокое обращение с детьми, нарушения интеллектуальной собственности, нарушения торговли товарами и услугами через электронные системы, терроризм и/или радикализм, сепаратизм и/или опасные незаконные организации, нарушения информационной безопасности, защиты прав потребителей, в сфере здравоохранения, контроля за наркотиками и продуктами питания; под «нарушением общественного порядка» подразумевается фальсифицированная информация и/или факты.

К организаторам электронных систем относят поставщиков услуг доступа в сеть «Интернет», поставщиков телекоммуникационных и сетевых услуг, поставщиков контента и поставщиков ссылок, которые предоставляют сети трафика электронной информации и/или электронных документов (п. 2 ст. 98 вышеуказанного Постановления Правительства Республики Индонезия). Прекращение / блокировка доступа (индонез. «pemutusan Akses») включает в себя прекращение соединения каналов, полное отключение сети/услуги и/или демонтаж оборудования (ст. 233 министерского решения № 5-2021 РИ), блокировку, закрытие учётной записи и/или удаление контента (пояснения к ст. 97 вышеупомянутого Постановления Правительства Республики Индонезия). Население может подать заявку на соответствующие действия министру. Соответствующие министерства и учреждения координируют с министром прекращение доступа; сотрудники правоохранительных органов могут направить соответствующий запрос министру; судебные учреждения — распорядиться о таковом (ст. 97 вышеупомянутого Постановления Правительства Республики Индонезия).

В КНР в 1998 г. была разработана система «Золотой щит», также известная как Великий Китайский файрволл или Великая китайская стена, для фильтрации контента. Китайское регулирование в части (не)правомерного контента можно

---

https://jdih.komdigi.go.id/produk_hukum/view/id/695/t/peraturan+pemerintah+nomor+71+tahun+2019+tanggal+10+oktober+2019 (дата обращения: 04.05.2025).

считать одним из самых обширных и включает Административные меры по защите безопасности Международной сети компьютерных информационных сетей; Положение о безопасности компьютерных информационных систем; Административные меры для информационных услуг в Интернете; Положение о защите права на распространение информационных сетей; Мнения о содействии здоровому и упорядоченному развитию мобильного Интернета, изданные Центральным комитетом Коммунистической партии Китая и Генеральным управлением Государственного совета; Циркуляр Государственного совета о уполномочивании Государственного управления Интернет-информации брать на себя ответственное управление информационным контентом в Интернете; Положение об управлении информационными услугами микроблогов; Положение об администрировании услуг Интернет-аудиовизуальных программ; Положение об управлении информационными услугами Интернет-новостей; Положение о работе по проведению интервью с подразделениями информационной службы Интернет-новостей; Правила реализации для управления лицензиями на информационные услуги в Интернете; Положение об управлении услугами онлайн-вещания в прямом эфире; Меры по административной защите авторского права в Интернете; Кодекс поведения при продвижении прямых трансляций Китайской рекламной ассоциации; Подробные правила стандартов цензуры для онлайн-короткого видеоконтента Китайской ассоциации служб сетевого вещания; Меры по маркировке синтетического контента, генерированного ИИ, Правила совместного использования правительственных данных, принятые в период с 2020 по 2025 гг.[559].

Отдельного внимания заслуживает вопрос о возможности **трансграничной передаче данных** (компетентными органами и юридическими лицами), в том числе

[559] AnJie Broad Law Firm. In brief: media law and regulation in China // Lexology. 11.06.2024. URL: https://www.lexology.com/library/detail.aspx?g=06005f86-e3e3-4106-8d55-736cf5da5e53 (accessed 19.05.2025); China further regulates AI-generated content // Allen and Gledhill. 02.04.2025. URL: https://www.allenandgledhill.com/publication/articles/30284/further-regulates-ai-generated-content?agreed=cookiepolicy (accessed 19.05.2025); 中华人民共和国国务院令 政务数据共享条例 [Приказ Государственного совета Китайской Народной Республики «Положение о предоставлении правительственных данных»] // Правительство КНР. URL: https://www.gov.cn/zhengce/content/202506/content_7026294.htm (дата обращения: 12.06.2025).

во исполнение ст. 40 Арабской Конвенции, Второго дополнительного протокола Будапештской конвенции, а также ряда руководств и рамочных программ АСЕАН.

Государство-участник Арабской конвенции может без получения разрешения от другого Государства-участника получать доступ к информации, доступной для общественности (из открытого источника), независимо от географического местоположения информации, а также с помощью информационных технологий на его территории получать доступ или саму информацию, обнаруженную в другом Государстве-участнике, при условии, что получено добровольное и юридически действительное согласие лица, имеющего законные полномочия раскрывать информацию.

Управление КСА по данным и искусственному интеллекту 05.05.2020 издало Национальную политику управления данными [560], регулирующую защиту персональных данных, порядок классификации информации [561], обмена и предоставления открытых или общедоступных (араб. «عام») данных, раскрытия ограниченной информации и передачи данных за пределы Королевства. Однако составляющие: ни политика обмена данными (араб. «سياسة مشاركة البيانات»), ни политика свободы информации (араб. «سياسة حرية المعلومات») — неприменимы для исполнения правовых запросов (с араб. «متطلبات قضائية» дословно судебные требования) и целей дознания (араб. «تحريات») или расследования (араб. «تحقيقات»). В Омане же подобное регулируется указом Султана Омана № 118 от 26.10.2011 (в ред. указа № 52-2022) «Закон о классификации государственных документов и регулировании охраняемых мест»[562], однако он не содержит положений касательно обмена данными. А указ Султана Омана № 6 от 09.02.2022 «Закон о защите

---

[560] سياسات حوكمة البيانات الوطنية [Национальная политика управления данными] // Управление КСА по данным и искусственному интеллекту. URL: https://sdaia.gov.sa/en/SDAIA/about/Documents/Policies005.pdf (дата обращения: 25.03.2025).

[561] Выделяются такие уровни тайны, как сиррийюн лилгаааяти или совершенно секретно/конфиденциально (дословно с араб. «سري للغاية» особо тайно), сиррийюн или секретный (дословно с араб. «سري») и мукайятун или ограниченный (араб. «مقيد»).

[562] قانون تصنيف وثائق الدولة وتنظيم الأماكن المحمية [указ Султана Оман № 118/2011 «Закон о классификации государственных документов и регулировании охраняемых мест»] // Онлайн база Кануун. URL: https://qanoon.om/p/2011/l2011118/ (дата обращения: 25.03.2025).

персональных данных» [563] не распространяется на случаи выявления или предотвращения любого уголовного преступления на основании официального письменного запроса от следственных органов (п. «و» ст. 3), хотя Исполнительным регламентом допускается возможность передачи данных напрямую во исполнение международного обязательства Султаната (решение Министра транспорта, связи и информационных технологий СО № 34 от 28.02.2024)[564].

На основании ст. 22 и 23 ФДЗ ОАЭ № 712 от 20.09.2021 «О защите персональных данных» [565] допускается трансграничная передача данных при условии одобрения Советом по данным, наличия применимого двустороннего или многостороннего соглашения касательно защиты персональных данных, уполномоченного органа и обеспечении адекватного уровня защиты. При отсутствии последнего передача всё равно возможна для целей международного судебного сотрудничества (араб. «تعاون قضائي دولي»). Именно «интересы» предупреждения, выявления, расследования и уголовного преследования правонарушения обычно являются исключением из общих правил при запрете трансграничной передачи данных, что указывается и в законодательстве азиатских стран (см., например, пп. «c» п. 1 раздела 17 Закона Республики Индия № 22 от 11.08.2023 «О защите цифровых персональных данных»[566]).

В ФДРЭ же при передаче в юрисдикцию третьей стороны (англ. «third party jurisdiction») — зарубежную страну, международную организацию и её подчиненные органы, регулируемые международным публичным правом, или в любой другой орган, созданный по соглашению между двумя или более странами

---

563 مرسوم سلطاني رقم ٦ / ٢٠٢٢ بإصدار قانون حماية البيانات الشخصية [указ Султана Оман № 6/2022 «Закон о защите персональных данных»] // Онлайн база Кануун. URL: https://qanoon.om/p/2011/l2011118/ (дата обращения: 02.05.2025).

564 وزارة النقل والاتصالات وتقنية المعلومات: قرار وزاري رقم ٣٤ / ٢٠٢٤ بإصدار اللائحة التنفيذية لقانون حماية البيانات الشخصية [Министерство транспорта, коммуникаций и информационных технологий: Министерское решение № 34/2024 об издании Исполнительного регламента Закона о защите персональных данных] // Онлайн база Кануун. URL: https://qanoon.om/p/2011/l2011118/ (дата обращения: 02.05.2025).

565 مرسوم بقانون اتحادي في شأن حماية البيانات الشخصية [Федеральный декрет-закон ОАЭ № 712 от 20.09.2021 «О защите персональных данных»] // Официальная база законодательства ОАЭ. URL: https://uaelegislation.gov.ae/ar/legislations/1972?keyword= (дата обращения: 25.03.2025).

566 The Digital Personal Data Protection Act No. 22 of 2023 // The Gazette of India Extraordinary. 2023. № 25.P. 1–21.

или на его основе, — требуется согласие только компетентного органа (Эфиопского управления телекоммуникаций, созданного на основании Прокламации ФДРЭ № 1148 от 12.08.2019[567]) при соблюдении адекватного уровня защиты, согласно Прокламации ФДРЭ № 1321 от 24.07.2024 «О безопасности персональных данных»[568].

На основании указа Министра юстиции, исламских дел и вакфа Королевства Бахрейн № 42 от 17.03.2022 «О передаче персональных данных за пределы Королевства Бахрейн» (далее — указ Министра юстиции, исламских дел и вакфа Королевства Бахрейн № 42-2022) [569] контролёр данных может передавать персональные данные непосредственно в страны и территории, указанные в Приложении к указу Министра юстиции, исламских дел и вакфа Королевства Бахрейн № 42-2022 (в число которых входит и РФ), без необходимости получения предварительного разрешения от Управления по защите персональных данных Королевства Бахрейн.

Если поставщик услуг получает приказ от компетентного суда или компетентного государственного органа иностранного государства, основанный на его юрисдикции в отношении контента клиента, то поставщик услуг должен как можно скорее в письменном виде сообщить Генеральному прокурору о таком приказе и предоставить ему копию такого приказа.

Компетентный судья и Генеральный прокурор Королевства, каждый в своём качестве, в соответствии с Законом Бахрейна № 60-2014 по запросу компетентного суда или государственного органа иностранного государства должны отдать приказ

---

[567] PROCLAMATION No. 1148/2019 PROCLAMATION FORCOMMUNICATION SERVICES // Ethiopian Communications Authority. URL: https://eca.et/wp-content/uploads/2024/05/Communications-Service-Proclamation-No.-1148-2019.pdf (accessed 02.05.2025).

[568] PROCLAMATION No. 1321/2024 PROCLAMATION TO PROVIDE FOR PERSONAL DATA PROTECTION // Ethiopian Communications Authority. URL: https://eca.et/wp-content/uploads/2024/10/personal_data_protection_proclamation_No_1321_2024.pdf (accessed 02.05.2025)

[569] Order (42) of 2022 of Ministry of Justice, Islamic Affairs and Waqf. Regarding the transfer of personal data outside the Kingdom of Bahrain // Ministry of Justice, Islamic Affairs and Waqf. URL: http://www.pdp.gov.bh/en/assets/pdf/executive-decisions/eng/trans-order-countries-and-territories-with-adequate-protection-en.pdf (accessed 25.03.2025).

об исполнении приказа, который является окончательным и не подлежит дальнейшему обжалованию, изданного таким судом или государственным органом в соответствии с его полномочиями по данному разделу, который касается предоставления доступа, раскрытия, сохранения или поддержания целостности контента клиента или любого вопроса в связи с контентом клиента, в отношении которого компетентный судья или Генеральный прокурор имеют полномочия в соответствии с указанным законом.

Расследование или обнаружение преступлений, уголовное преследование, исполнение приговора могут выступать в качестве целей-исключений по передаче сведений за пределы КСА при отсутствии соблюдения соответствующего уровня защиты, установленных Саудовским управлением по данным и ИИ, за исключением случаев, когда затрагиваются национальные или жизненно важные интересы Королевства, высоких рисков и при невозможности обеспечения сохранности данных со стороны контролирующего органа (ст. ст. 6 и 7 Исполнительных правил к Положению КСА от 16.09.2021 «О защите персональных данных» в ред. от 27.03.2023[570]).

В странах Юго-Восточной Азии предлагается имплементировать и руководствоваться механизмом трансграничных потоков данных АСЕАН 2019 г.[571], входящим в состав Рамочной программы по управлению данными, разработанных в рамках Рамочной программы по управлению цифровыми данными TELMIN 2018 г. [572] . Указанный механизм имеет две составляющие, типовые договорные

---

[570] اللائحة التنفيذية لنظام حماية البيانات الشخصية [Исполнительные правила к Положению о защите персональных данных] // Национальная платформа управления данными КСА. URL: https://dgp.sdaia.gov.sa/wps/portal/pdp/knowledgecenter/details/PDPL2/!ut/p/z1/jY-xDoIwFEW_xQ8gfS1Q61gEIgpaUkDsYhgESbQQQxz8ehsGB6Pi215yTu69SKESKV3d26Ya2k5XF_MfFD2S1OfYczAWpAiBcpZmxS4lcuGi_QhEPKArLIEIurWBspTZLJgDgIvUPz58OQ5T_noKMAvILVkmDVJ9NZytVtcdKoUvYmLC1ai_6mOcM1M_2dAszDF4zjvwYd8I_BggTxr117x8xLWMLD57As174Bg!/dz/d5/L0lHSkovd0RNQU5rQUVnQSEhLzROVkUvYXI!/ (дата обращения: 10.05.2025).

[571] ASEAN Data Management Framework // ASEAN. URL: https://asean.org/wp-content/uploads/2021/08/ASEAN-Data-Management-Framework.pdf (accessed 03.05.2025).

[572] ASEAN TELECOMMUNICATIONS AND INFORMATION TECHNOLOGY MINISTERS MEETING (TELMIN) FRAMEWORK ON DIGITAL DATA GOVERNANCE // ASEAN. URL: https://asean.org/wp-content/uploads/2012/05/6B-ASEAN-Framework-on-Digital-Data-Governance_Endorsedv1.pdf (accessed 03.05.2025).

положения АСЕАН и сертификация АСЕАН для трансграничных потоков данных. Они нацелены на субъекты малого и среднего предпринимательства для развития цифровой экономики и унификации процессов. В 2020 г. были выработаны руководящие принципы, утверждённые ADGMIN[573], для соблюдения Рамочной программы по защите персональных данных 2016 г. и иных стандартов по типу Рамочной программы конфиденциальности АТЭС или Руководства по конфиденциальности ОЭСР. Как указывается в перечисленных документах, выстраивание связи между субъектами (тот, кто контролирует данные, и тот, кто обрабатывает их) должно основываться на обеспечении адекватного уровня защиты, ясных и чётких требованиях законодательства страны, пересмотру и снижению ограничений избыточных политик по хранению данных в государстве (по принципу локализации данных) или условий по передаче из страны происхождения (в том числе согласие индивида).

Несмотря на то, что ни в одном из рассматриваемых документов нет упоминания о передаче данных для целей уголовного преследования, способствование единообразию регулирования и подхода в частном секторе упрощает процедуры и повышает прозрачность при запросах любого рода, в том числе для целей уголовного судопроизводства. Вдобавок возможность трансграничной передачи данных нужно соотносить с концепцией цифрового суверенитета государства и локализацией данных (как правительственных, так и персональных). Страны Глобального Юга в подходах к определению подобного разнятся.

Итак, с точки зрения уголовно-процессуальных мер противодействия киберпреступлениям особую важность представляют доказывание (в частности, правовой статус и порядок получения цифровых / электронных доказательств), наложение замораживания, ареста и конфискации в целях обеспечения

---

[573] 1st ASEAN DIGITAL MINISTERS' MEETING (ADGMIN) 2020 IMPLEMENTING GUIDELINES FOR ASEAN DATA MANAGEMENT FRAMEWORK AND ASEAN CROSS BORDER DATA FLOWS MECHANISM // ASEAN. URL: https://asean.org/wp-content/uploads/2021/08/Implementing-Guidelines-for-ASEAN-Data-Management-Framework-and-Cross-Border-Data-Flows.pdf (accessed 03.05.2025).

сохранности активов (имущества) и возмещения ущерба, использование электронного документооборота и ИТ для оптимизации, упрощения и процессуальной экономии в рамках уголовного судопроизводства, блокировка или ограничение доступа к Интернет-ресурсам, содержащим деструктивный контент, а также возможность передачи сведений за рубеж, минуя традиционный порядок получения взаимной правовой помощи по уголовным делам через запросы в центральные органы по дипломатическим и иным каналам.

Опуская полемику в части терминологии (см. Приложение № 8), отметим: в то время как в странах Аравийской зоны (и некоторых аль-Магриба) цифровые доказательства судебной практикой признавались в качестве таковых ещё до их законодательного закрепления, в отдельных случаях (например, Тунис) их правовой статус до сих пор не определен. Фактически он может может быть сведён к трем подходам: самостоятельный вид, носитель информации, приравненный к письменному документу, вещественное доказательство, полученное в ходе судебно-медицинской экспертизы.

При этом с учётом круга (не)гласных следственных действий и незакрытого перечня нет законодательно[574] жёсткой «привязки» к привлечению специалиста (эксперта)[575], что несколько отличается от отечественной практики. Помимо того, что не проводят различий между ними, в России созданы криминалистический и судебно-экспертный центры при Следственном комитете России, экспертно-криминалистический центр МВД России, Институт криминалистики ФСБ России, на которые возлагается основная нагрузка по анализу, в то время как в зарубежных странах, в частности в арабских и африканских, в указанных целях допускается привлечение сотрудников министерств и подведомственных учреждений

---

[574] На самом деле это касается не только нормативных правовых актов. Исходя из т.н. белых книг, составленных представителями науки и правоприменителями, указанных в § 2 Главы 2, предполагается, что прокурор или полицейский должны быть технически подкованы и иметь соответствующую квалификацию или хотя бы минимальные «представления» о специфике цифровых следов.

[575] Эксперты скорее работают с т.н. статикой, хранящейся на изъятом материальном носителе, в то время как специалисты — с «динамикой», содержащейся в Интернет-пространстве.

(представителей исполнительной власти)[576]. Как одной из важных составляющих следственных действий и средства формирования доказательств выступает фото- и видеофиксация [577], а также искусственный интеллект как вспомогательный инструмент по поиску, обнаружению, фиксации и сохранности криминалистически значимой информации в электронной форме.

Тем не менее большинство рассматриваемых государств признаёт их и имеет довольно схожие процедуры по их получению: обыск, выемка, изъятие, перехват, прослушивание, контроль сообщений / контента, электронный мониторинг, дистанционные и физические цифровые расследования, извлечение и копирование данных. Их классификация как на доктринальном, так и на законодательном уровнях значительно разнится. В ряде случаев (Индия и Арабский Восток) для сохранности электронных доказательств разработаны подробные руководства подобно пошаговым инструкциям. С учётом новых возникающих киберугроз и развития технологий ИИ и мета-вселенной представляется важным изучать передовые подходы (в частности, использование AI) и модернизировать или адаптировать традиционные под виртуальную реальность.

Действующим зарубежным законодательством охватываются различные виды данных, хранимых поставщиками услуг, в том числе о содержании (контенте), о трафике, учете преобразования частных сетевых адресов в публичные сети, конечном оборудовании, технических характеристиках, дате, времени и продолжительности соединения, дополнительных услугах, посещённых Интернет-ресурсах, идентификационные (регистрационные) сведения, а также связанные с

---

[576] О первом в части РФ см. Бастрыкин А. И. Цифровые технологии современной криминалистики // Вестник Академии Следственного комитета Российской Федерации. 2021. № 2 (28). С. 11-17.
О втором раскрыто в § 2 Главы 2: подобное выводится из системного толкования, либо напрямую указывается в уголовно-процессуальном регулировании (e.g., п. 1 ст. 6 Закона Республики Индонезия № 8 от 31.12.1981 «Уголовно-процессуальный кодекс»). Undang-undang (UU) Nomor 8 Tahun 1981 tentang Hukum Acara Pidana [Закон Республики Индонезия № 8 от 31.12.1981 «Уголовно-процессуальный кодекс»] // Законодательная база Республики Индонезия. URL: https://peraturan.bpk.go.id/Details/47041/uu-no-8-tahun-1981 (дата обращения: 10.02.2025).

[577] В случае с электронными доказательствами также производится фиксация посредством снятия скриншотов, хотя стоит отметить, что с учётом развития технологий дип-фэйка подобное может оказаться малополезным или даже бессмысленным.

периферийными устройствами связи и с географическим местоположением пользователя. Срок варьируется в среднем от полутра месяца – полугода до двух лет. Их сохранение чаще осуществляется по приказу прокуратуры, нежели по судебному решению (в зависимости от необходимости получения доступа и типа сведений). Обеспечение процесса извлечения данных может возлагаться как на компетентные правоохранительные органы или специализированные организации, так и на сотрудников юридического лица, подлежащего обыску (выемке). Отказ от сотрудничества может влечь за собой наложение юридической ответственности, вплоть до уголовной.

С учётом расширения понятия места совершения преступления возникают предпосылки для конфликта юрисдикций (на межгосударственном уровне), подсудности и подследственности (на внутригосударственном уровне) и, как следствие, для развития новых юрисдикционных привязок.

Понятие имущества, полученного преступным путём, может охватывать и виртуальные активы с учётом широких формулировок понятийного аппарата, однако в доктрине и на практике вызывают споры соотнесения объекта регулирования и вида актива. В то время как общеуголовно-процессуальными и антиотмывочными законами на федеральном (государственном) уровне могут быть предусмотрены запреты и/или могут отсутствовать процедуры, специфические для изъятия виртуальных активов, в САР и ОЭЗ (СФЗ) разработано прогрессивное регулирование. С учётом особых институциональных механизмов, освещённых в § 2 Главы II, предположим возможность оперативного реагирования, сбора и передачи информации о возможном преступлении и расследовании (производстве первоначальных следственных действий), которые способствуют, как следствие, оперативному наложению обеспечительных мер, которые включают арест, замораживание и конфискацию. В зависимости от рассматриваемой юрисдикции порядок может быть судебным, внесудебным (административным) и смешанным (с условием [578] или без наличия обвинительного приговора). Межгосударственное

[578] Примеры — Индия и Индонезия.

взаимодействие осуществимо в значительной мере через механизм ВПП по УД (исключением является Индонезия). Основанием для взаимодействия выступают универсальные, региональные, двусторонние международные договоры, принцип взаимности, который может специфически обозначаться в отдельных странах, а также национальное уголовно-процессуальное, антикоррупционное и антиотмывочное законодательство. Центральный орган, как и компетентные органы, могут различаться именно для исполнения запросов по наложению ограничительных мер в рамках национального регулирования и при присоединении (подписании и ратификации) международных договоров (исключением является КНР). Подробность регламентации процедур разнится даже в рамках одного региона.

Ряду государств (e.g., ФДРЭ, Индонезии, КБ, Кувейту, Катару, СО, ИРИ) требуется более чётко определить стандарты медиаконтента, которые выявляются путём только системного толкования ряда источников смежных отраслей права, и определить процедуры для ограничений в случае выявления нарушений. Несмотря на активное внедрение ИТ и успешную цифровую трансформацию отдельных стран (ОАЭ, КСА, ИРИ), всё же предстоит ещё долгий путь для того, чтобы констатировать одинаковый или приблизительно схожий высокий уровень автоматизации или цифровизации процессов. В отдельных случаях (e.g., Республика Индонезия) ещё до принятия соответствующих поправок в законодательстве или в отсутствие вообще такового (e.g., КСА) внедряются технологии, что, с одной стороны, отвечает объективным потребностям при отправлении правосудия (видеоконференцсвязь) или развития экономики (ИИ и Интернет вещей при управлении городом), с другой — порождает правовую неопределённость при действительности процедур по получению доказательств и пробелы при будущем установлении ответственных лиц.

Случаи, где регулированием предусмотрен порядок наложения подобной процессуальной меры (участие прокуратуры, суда или органов исполнительной власти), в некоторой степени сходны с российским правопорядком. Вопрос о трансграничной передаче данных находится только на промежуточной стадии

развития, охватывая гражданские и гражданско-процессуальные нормы, а также типовые оговорки (особенно в рамках региональных объединений). В большинстве законов стран Глобального Юга не предусмотрены процедуры непосредственно для целей уголовного преследования, однако есть и исключения (e.g., Королевство Бахрейн).

ГЛАВА IV. МЕЖДУНАРОДНОЕ СОТРУДНИЧЕСТВО В СФЕРЕ ПРОТИВОДЕЙСТВИЯ КИБЕРПРЕСТУПЛЕНИЯМ МЕЖДУ РОССИЙСКОЙ ФЕДЕРАЦИЕЙ И ОТДЕЛЬНЫМИ СТРАНАМИ ГЛОБАЛЬНОГО ЮГА

§ 1. Основы международного сотрудничества в сфере противодействия киберпреступлениям между Российской Федерацией и отдельными странами Глобального Юга

С доктринальной точки зрения международное сотрудничество в сфере борьбы [579] с преступностью (в целом) и с отдельными видами преступлений международного характера (как частный случай) охватывает 10 направлений (организационно-правовых форм), корреспондирующих национальному и региональному уровням:

1) *принятие согласованных мер по установлению на международно-правовом* (универсальном и региональном) *уровнях преступности и наказуемости определенных общественно-опасных деяний, вызывающих озабоченность человечества,* что корреспондирует криминализации и пенализации на национальном уровне и является порой следствием указанных явлений;

2) *разработка и заключение* международных договоров, *принятие других международно-правовых документов в качестве правовой основы совместной деятельности государств и международных организаций, их органов в сфере борьбы с преступностью, а также регламентирующих порядок осуществления полномочий в этой сфере, процессуальный порядок отправления международного правосудия и сотрудничества государств в борьбе с преступностью*;

3) *учреждение и формирование* на договорной и иной международно-правовой основе *организаций и/или их органов, осуществляющих свою*

---

[579] Отметим: в то время как в доктрине и российском законодательстве проводится различие между борьбой, противодействием, профилактикой и предупреждением, в отдельных случаях термины могут использоваться как взаимозаменяемые, близкие по смыслу и вызывают споры при избрании наиболее подходящего. Подобное указывается в замечаниях на второй сессии по разработке Универсальной конвенции: англ. counter, prevent and combat. См. подробнее A/AC.291/CRP.8/Rev.1 // UNODC. URL: https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Second_session/CRP8_Rev1.pdf (accessed 21.04.2025).

деятельность в сфере борьбы с преступностью, а также международных уголовных судов;

4) *обеспечение пресечения готовящихся или совершенных преступлений*, в том числе путем координации, организации и проведения в необходимых случаях оперативно-розыскных мероприятий, а также оказания содействия в сфере правоохранительной деятельности;

5) *сотрудничество в сфере уголовного судопроизводства* охватывает вопросы, связанные с осуществлением уголовного преследования, отправлением правосудия и исполнением приговоров;

6) *деятельность органов международной уголовной юстиции по привлечению к ответственности лиц, виновных в совершении международных преступлений, отправлению правосудия по делам о них, осуществлению уголовного преследования и наказанию виновных лиц*;

7) *пенитенциарное сотрудничество*, в том числе исполнение уголовных наказаний, назначенных органами международной уголовной юстиции лицам, виновным в совершении международных преступлений, приговоров иностранных судов, а также сотрудничество в сфере выработки и реализации международных стандартов обращения с лицами, содержащимися под стражей, мер наказания, не связанных с заключением под стражу, и реституционного правосудия;

8) *сотрудничество в сфере постпенитенциарного воздействия*;

9) *выработка стандартов предупреждения преступности, обращения с правонарушителями, уголовной юстиции, а также координация деятельности по борьбе с преступностью на международном уровне*;

10) *межгосударственное оказание* материальной, профессионально-технической, научной, образовательной, экспертной и иной *помощи в борьбе с преступностью*.

Исходя из указанных направлений, необходимо рассмотреть три составляющих: акты мягкого права и юридически обязательные документы как правовую основу, институциональные механизмы и порядок их взаимодействия в

рамках региональных объединений и организаций БРИКС, ШОС, ЛАГ, ОИС, ССАГПЗ, АС, IGAD и АСЕАН.

С учётом расширений БРИКС с 01.01.2024 участниками стали АРЕ, ОАЭ, ФДРЭ, ИРИ (КСА так и не приняли приглашение до сих пор), а с 01.01.2025 — Республика Индонезия особую значимость приобретает учрежденный институциональный механизм по противодействию киберпреступлениям — рабочая группа БРИКС по вопросам безопасности в сфере использования ИКТ. С правовой же точки зрения взаимодействие выражается в составлении общих руководящих документов: Коммюнике министров связи стран БРИКС по итогам встречи «Расширение сотрудничества в сфере телекоммуникаций и информационно-коммуникационных технологий» от 23.10.2015, Дорожная карта практического сотрудничества БРИКС в обеспечении безопасности в сфере использования ИКТ, упомянутой в Сямэньской декларации руководителей стран БРИКС (Сямэнь, КНР, 04.09.2017), Антитеррористическая стратегия БРИКС 2020 г.[580], Йоханнесбургская декларация-II «БРИКС и Африка: партнёрство в интересах совместного ускоренного роста, устойчивого развития и инклюзивной многосторонности» (Йоханнесбург, ЮАР, 23.08.2023), Казанская декларация «Укрепление многосторонности для справедливого глобального развития и безопасности» (Казань, РФ, 23.10.2024), Совместная декларация 15-й Встречи министров торговли, содержащее как приложение Соглашение по управлению цифровой экономикой (Бразилиа, ФРБ, 21.05.2025), Декларация «Укрепление сотрудничества Глобального Юга для более инклюзивного и устойчивого управления» (Рио-де-Жанейро, ФРБ, 06.07.2025) (далее — Декларация Рио-де-Жанейро), Декларация «Глобальное управление искусственным интеллектом» (Рио-де-Жанейро, ФРБ, 07.07.2025)[581]. Как отмечается в Декларации Рио-де-

[580] Зиновьева Е., Игнатов А. БРИКС в глобальном режиме ИКТ-безопасности // Международные процессы. 2023. № 21 (4). С. 104-132.

[581] В последних трех документах также впервые на уровне БРИКС встречаются термин «Глобальный Юг». См. подробнее Цыплакова А.Д. Концептуализация понятия «(страны) Глобального Юга»: диффузия повседневной речи, научной терминологии и специализированных дискурсов в призме лингвокультурологии // Концепт: философия, религия, культура. 2025. № 9 (2). С. 116-134; JOINT DECLARATION OF THE 15th BRICS TRADE MINISTERS MEETING //

Жанейро, формами взаимодействия выступают обмены информацией и стратегиями, совместные исследования и разработки, сотрудничество правоохранительных органов и CERT (п. п. 36, 40). По вопросам же уголовного судопроизводства сотрудничество носит скорее двусторонний или неформальный характер.

На сегодняшний день, к сожалению, ряд международных договоров, в рамках которых возможно осуществление отдельных видов международного сотрудничества в сфере уголовного судопроизводства и правоохранительного содействия, не могут выступать в качестве правовой основы для взаимодействия. Так, в рамках ШОС сотрудничество по преступлениям в сфере информационных технологий предусмотрено Соглашением о сотрудничестве между правительствами государств-членов Шанхайской организации сотрудничества в борьбе с преступностью (Ташкент, 11.06.2010) [582], однако значительная часть рассматриваемых государств не являются подписантами указанного документа. Вдобавок Российская Федерация не является подписантом Будапештской конвенции (в отличие от представителей Северной Африки).

Российская Федерация не входит в состав таких международных организаций и объединений, как ЛАГ, ОИС, ССАГПЗ, АС, IGAD и АСЕАН, хотя в их рамках сформирована обширная база, регламентирующая, например, порядок выдачи для уголовного преследования и/или исполнения приговора, оказания взаимной правовой помощи по уголовным делам и передачи осуждённых, а также различные структурные подразделения и органы с самостоятельной правосубъектностью по

Brazilian Government. URL: https://www.gov.br/mdic/pt-br/centrais-de-conteudo/publicacoes/brics/comercio/ingles/brics_tmm_package_of_outcomes_v21-05-25_final-version.pdf (accessed 12.06.2025); Декларация Рио-де-Жанейро «Укрепление сотрудничества Глобального Юга для более инклюзивного и устойчивого управления» (Рио-де-Жанейро, Бразилия, 06.06.2025) // Кремль: официальный сайт. URL: http://static.kremlin.ru/media/events/files/ru/gvTArkWauqwuryk9xzLt3HuuI7EBmqrC.pdf (дата обращения: 06.07.2025); Leaders' Declaration on Global Governance of Artificial Intelligence // BRICS. URL: https://brics.br/en/documents/presidency-documents/250706_brics_ggai_declarationfinal.pdf (accessed 07.07.2025).

[582] Соглашение о сотрудничестве между правительствами государств-членов Шанхайской организации сотрудничества в борьбе с преступностью (Ташкент, 11.06.2010) // Шанхайская организация.

типу АСЕАНАПОЛ, АФРИПОЛ, Организации сотрудничества начальников полиции Восточной Африки (англ. «EAAPCO»), Полицейской службы Совета сотрудничества арабских государств Персидского залива (англ. «GCC-Pol», араб. «جهاز الشرطة الخليجية»), Центра информации по уголовным делам по борьбе с наркотиками Совета сотрудничества арабских государств Персидского залива по линии полицейского сотрудничества (англ. «GCC-CICCD», араб. « مركز المعلومات الجنائية لمكافحة المخدرات لمجلس التعاون لدول الخليج العربية»). Тем не менее все они подключены к системе Интерпол «I-24/7».

Несмотря на то, что РФ является государством-наблюдателем ОИС, оно не может в полной мере пользоваться привилегиями члена, в частности участвовать в оперативной деятельности или обмене информацией в рамках Центра Организации исламского сотрудничества по координации и сотрудничеству полиции (англ. «OICPOL», араб. «مركز منظمة التعاون الإسلامي للتنسيق والتعاون الشرطي») (ст. 9 Основного положения ОИСПОЛ) [583] . Подобный подход характер67 для большинства организаций, объединений и органов в части партнёрства по диалогу или статуса наблюдателя. Схожую параллель можно провести, например, с наблюдателями АСЕАНАПОЛ: ОАЭ и GCC-Pol, которым позволительно участвовать во встречах контактных лиц (офицеров связи) и связанных мероприятиях, а также во встречах глав делегаций без права на выступления.

Российское взаимодействие с указанными организациями и объединениями происходит в формате саммитов, консультаций на уровне министерств и специализированных ведомств. Например, действуют консультации глав ведомств АСЕАН по вопросам наркотиков и транснациональной преступности плюс Россия (англ. «ASEAN Senior Officials on Drug Matters (ASOD) Plus Russia Consultation and the Senior Officials Meeting on Transnational Crime (SOMTC) Plus Russia Consultation»). Их взаимодействие затрагивают вопросы неправомерного использования Интернета, цифровых валют и онлайн-магазинов для преступных

[583] النظام الأساسي لمركز منظمة التعاون الإسلامي للتنسيق والتعاون الشرطي [Основное положение Центра Организации исламского сотрудничества по координации и сотрудничеству полиции] // Организация исламского сотрудничества. URL: https://www.oic-oci.org/upload/pages/conventions/ar/oic_policy_5893427_ar.pdf (дата обращения: 09.03.2025).

целей[584]. Несмотря на то что в Декларациях российско-африканских саммитов киберпреступления не выделялись в качестве направления по линии сотрудничества в сфере безопасности, отмечалось важность разработки и принятия Универсальной конвенции для предотвращения использования ИКТ в преступных целях, в том числе для подрыва суверенитета, нарушения территориальной целостности государств, проведения компьютерных атак на критическую информационную инфраструктуру, а также в террористических, экстремистских и иных преступных целях[585].

На двустороннем уровне отметим подписание договоров и меморандумов по отдельным направлениям МССУС, оперативному обмену информацией между подразделениями финансовой разведки и правоохранительными органами, а также формирование соответствующих органов для обеспечения безопасности. Примерами могут служить совместный комитет для эффективного выполнения положений Соглашения о безопасности между Федеративной Демократической Республикой Эфиопия и Республикой Йемен (Аддис-Абеба, 03.10.1999)[586], а также Центр сотрудничества полиции на основании Соглашения между правительством

---

[584] Statement of ASEAN and the Russian Federation on Cooperation against Illicit Drugs Trafficking // ASEAN. URL: https://asean.org/wp-content/uploads/2021/10/81.-ASEAN-Russia-Statement-on-Drug-Cooperation-Final.pdf (accessed 26.04.2025).

[585] Joint Statement of the First Ministerial Conference of the Russia-Africa Partnership Forum (Russian Federation, Sirius Federal Territory, 10 November 2024) // Ministry of Foreign Affairs of the Russian Federation. 11.11.2024. URL: https://mid.ru/en/foreign_policy/russia_africa/1980876/?TSPD_101_R0=08765fb817ab2000e9e9350fe5b8ccad71e28b5b34d25b5ceb354a2614c292c2c81296e5b08e326e08b689aaa314300074c1e3f0fd4936a874f19ee6d306dd95051157b166e461d6e2a00f731a052eae620f184963a6cb310125e45db20133e7 (accessed 26.04.2025); Declaration of the Second Russia–Africa Summit // Summit Africa. URL: https://summitafrica.ru/en/about-summit/declaration-2023/ (accessed 26.04.2025); Declaration of the First Russia–Africa Summit // Summit Africa. URL: https://summitafrica.ru/en/about-summit/declaration/ (accessed 26.04.2025); Declaration of the Second Russia–Africa Summit on Cooperation in the Field of International Information Security - Russia-Africa Summit // Ministry of Foreign Affairs of the Russian Federation. URL: https://oldrussianembassyza.mid.ru/russia-africa-summit/-/asset_publisher/SWhrwjfrWDXU/content/declaration-of-the-second-russia-africa-summit-on-cooperation-in-the-field-of-international-information-security?TSPD_101_R0=08765fb817ab20004bbd9a141c8b68ad300f15a9104506ad179abed1ff184d18e2edab1fac2ba1e7084e61ec07143000716877089 6f014c47d66242242761410f33c7a65277afbcfaef22b918b45646cbdeb612134e9e69902f04a44594f375b (accessed 26.04.2025).

[586] اتفاقية اليمن وإثيوبيا- اتفاق امني [Соглашение между Йеменом и Эфиопией — Договор о безопасности] // Генеральная прокуратура Республики Йемен. URL: http://agoyemen.net/lib_details.php?id=207 (дата обращения: 20.04.2025).

Королевства Испания и правительством Королевства Марокко о трансграничном сотрудничестве полиции (Мадрид, 16.11.2010)[587], совместный комитет согласно меморандуму о взаимопонимании между Главным управлением безопасности информационных систем Королевства Марокко и Советом по кибербезопасности ОАЭ от 19.10.2023[588]. Соглашением о безопасности между ФДРЭ и Республикой Йемен регулируются вопросы не только правоохранительного содействия, технического и научного сотрудничества, но и реализации выдачи, передачи лиц и имущества. Тем не менее подобная практика почти не встречается при осуществлении взаимодействия между Российской Федерацией и отдельными государствами Глобального Юга. Например, 15.04.2025 был подписан Дополнительный протокол к Меморандуму между Генеральной прокуратурой РФ и Генеральной прокуратурой ОАЭ от 20.12.2021, согласно которому будет создана рабочая группа по противодействию преступности и защите прав граждан[589].

Отдельного внимания заслуживает Универсальная конвенция и позиции государств при её разработке. Отметим особую активность при официальных

---

[587] Примечательно, что подобное соглашение было заключено раньше, чем Соглашение о сотрудничество в сфере борьбы с преступностью между указанными странами (13.02.2019). См. подробнее Acuerdo entre el Gobierno del Reino de España y el Gobierno del Reino de Marruecos en materia de cooperación policial transfronteriza, hecho "ad referendum" en Madrid el 16 de noviembre de 2010 // Boletín official del estado. 2012. № 116. Sec. I. P. 35412–35416; Convenio entre el Reino de España y el Reino de Marruecos sobre cooperación en materia de seguridad y de lucha contra la delincuencia, hecho en Rabat el 13 de febrero de 2019 // Boletín official del estado. 2022. № 83. Sec. I. P. 46756–46760.

[588] MOROCCO AND THE UNITED ARAB EMIRATES HAVE SIGNED A MEMORANDUM OF UNDERSTANDING (MOU) WITH THE AIM OF ENHANCING THEIR COOPERATION IN CYBERSECURITY // DGSSI. URL: https://www.dgssi.gov.ma/en/evenements/morocco-and-united-arab-emirates-have-signed-memorandum-understanding-mou-aim-enhancing (accessed 24.05.2025).

[589] Игорь Краснов подписал с Генеральным прокурором Объединенных Арабских Эмиратов Хамадом Саифом Аль-Шамси дополнительный протокол о создании рабочей группы по противодействию преступности и защите прав граждан // Генеральная прокуратура: официальный сайт. 15.04.2025. URL: https://epp.genproc.gov.ru/web/gprf/mass-media/news?item=102347932 (дата обращения: 26.04.2025).

заявлениях и позициях РФ[590], ИРИ[591], Индии и отдельных арабских стран (АРЕ, СО), а также рассматриваемых организаций АСЕАН, АС. Подчёркивалась вовлечённость гражданского общества и частного сектора[592].

На первой сессии (28.02–11.03.2022) государства Глобального Юга высказали следующие позиции. В части предупреждения КНР отдавала предпочтение профилактическим мерам, назначению специализированных учреждений и разработке обязанностей частного сектора, выступала за криминализацию и пенализацию проникновения на объекты ИКТ-инфраструктуры и КИИ, кибервымогательства, кибермошенничества, киберпорнографии, участие в темной производственной цепочке, нарушение авторских и смежных прав с использованием ИТ, использование Интернета в террористических целях или распространения вредоносной информации. Китай отмечал, что лишь факт передачи данных на территории государства не может быть достаточным основанием для осуществления юрисдикции, а также предлагал осуществлять трансграничный сбор электронных доказательств с уважением государственного суверенитета[593].

АРЕ делала упор на признание преступным неправомерного использования информационно-коммуникационных услуг и технологий, превышения прав доступа, кибератаки, кибермошенничества и кибервымогательства, незаконных

---

[590] Russian Federation (27 May 2020) // UNODC. URL: https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Comments/Russian_Federation.pdf (accessed 20.04.2025); Joint comment by Angola, Azerbaijan, Belarus, Burundi, Cambodia, China, Congo, Cuba, Democratic People's Republic of Korea, Eritrea, Ethiopia, Iran (Islamic Republic of), Kazakhstan, Kyrgyzstan, Lao People's Democratic Republic, Madagascar, Myanmar, Nicaragua, Pakistan, Russian Federation, Sudan, Suriname, Syrian Arab Republic, Tajikistan, Togo, Venezuela (Bolivarian Republic of) and Zimbabwe (9 February 2021) // UNODC. URL: https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Comments/RF_9_February_2021.pdf pdf (accessed 20.04.2025).

[591] Iran (Islamic Republic of) (20 April 2020) // UNODC. URL: https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Comments/Iran.pdf (accessed 20.04.2025).

[592] Egypt (30 June 2020) // UNODC. URL: https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Comments/Egypt.pdf (accessed 20.04.2025).

[593] 中国对联合国打击为犯罪目的使用信通技术公约 范围 [Вклад Китая в Конвенцию Организации Объединенных Наций против использования ИКТ в преступных целях] // УНП ООН. URL: https://www.unodc.org/documents/Cybercrime/AdHocCommittee/First_session/Comments/Chinas_Suggestions_on_the_Scope_Objectives_and_Structure_AHC.pdf (дата обращения: 21.04.2025).

использований электронных средств платежа, преступлений с использованием ИКТ или их использования для совершения деяний: фальсификации, побуждения или принуждения к совершению самоубийства, вовлечения несовершеннолетних в преступную деятельность, нарушения права на неприкосновенность, террористические и финансовые преступления, транснациональной организованной преступности[594].

ИХК дополнила бы список слежкой за потоком данных; ПО, кодами доступа и аппаратными средствами для дешифровки; распространением ложных новостей, расовой дискриминацией, эксплуатацией женщин и жестоким обращением с ними; незаконной торговлей через Интернет; оскорблением религий, стран и символов; электронным фишингом и призывами к мятежу, подстрекательством или распространением ненавистнической риторики [595]. Султанат Оман отмечал необходимость уголовно-правового запрета на использование ИКТ при нападениях на гражданские объекты, особенно критически важной инфраструктуры[596].

С точки зрения уголовного процесса отмечалась важность закрепления статуса цифровых доказательств. Государство Кувейт ратовало за использование существующих информационных сетей с назначением контактных лиц для целей конвенции[597].

---

[594]Позиция была повторена и на третьей сессии. عناصر ورقة من جانب جمهورية مصر العربية مقدمة اتفاقية دولية شاملة في إطار الأمم المتحدة في إطار بلورة مكافحة استخدام تكنولوجيا الاتصالات والمعلومات لأغراض إجرامية [Элементы документа Арабской Республики Египет, представляющего всеобъемлющую международную конвенцию в рамках Организации Объединенных Наций по борьбе с использованием информационно-коммуникационных технологий в преступных целях] // УНП ООН. URL: https://www.unodc.org/documents/Cybercrime/AdHocCommittee/First_session/Comments/Egypt_AHC_comments.pdf (дата обращения: 21.04.2025).

[595] Позиция была повторена и на второй сессии. المملكة الأردنية الهاشمية اتفاقية شاملة بشأن مكافحة استخدام تكنولوجيا المعلومات والاتصالات للأغراض الإجرامية [Иорданское Хашимитское Королевство. «Всеобъемлющая конвенция о борьбе с использованием информационно-коммуникационных технологий в преступных целях»] // УНП ООН. URL: https://www.unodc.org/documents/Cybercrime/AdHocCommittee/First_session/Comments/Jordan_AHC_Views_on_the_new_convention.pdf (дата обращения: 21.04.2025).

[596] Kuwait (17 September 2021) // UNODC. URL: https://www.unodc.org/documents/Cybercrime/AdHocCommittee/First_session/Comments/Oman_18_Oct_2021.pdf (accessed 21.04.2025).

[597] Oman (18 October 2021) // UNODC. URL: https://www.unodc.org/documents/Cybercrime/AdHocCommittee/First_session/PM.SK.cm.166.2021.pdf (accessed 21.04.2025).

Республика Индонезия поощряла использование ИКТ в мирных целях и поддерживала общий подход по криминализации и пенализации[598]. Республика Индия же — борьбу с транснациональными киберпреступными операциями[599].

На второй сессии (30.05–10.06.2022) Египет представил собственное видение терминологии, значительно шире итогового документа, в частности личный кабинет, электронная почта, фиксация, сайт, цифровые доказательства[600] и администратор сайта, а также представления о следственных действиях, которые повторяли национальные положения или были сходны с ними[601]. Иран отмечал важность защиты суверенитета[602]. Республика Индия выступала за криминализацию кибертерроризма, а также предлагала специфические юрисдикционные принципы — юрисдикция, основанная на данных (англ. «Data Oriented Jurisdiction»).

Юрисдикция, ориентированная на данные, означает, что юрисдикция страны, данные граждан которой хранятся / обрабатываются / скринируются / федерализуются в любой точке мира, должна превалировать в отношении данных, независимо от места их физического хранения / обработки / скрининга / федерализации. Подобный подход обеспечит первичность права собственности на данные и вопрос неприкосновенности частной жизни (признанное

---

598 Indonesia's Submissions // UNODC. URL: https://www.unodc.org/documents/Cybercrime/AdHoc Committee/First_session/Comments/Indonesias_input_AHC.pdf (accessed 21.04.2025).

599 UN Ad Hoc Committee (AHC) to elaborate a comprehensive International Convention on countering the use of Information and Communications Technologies for criminal purposes. Indian views on Scope, Objectives and Structure 6th December, 2021 // UNODC. URL: https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Comments/India_-_Views_on_scope_objective_and_structure_7.12.2021_1.pdf (accessed 21.04.2025).

600 В официальном первичном и дополненном заявлениях в качестве равнозначных использовались термины «цифровое доказательство» и «электронное доказательство».

601 عناصر ورقة من جانب جمهورية مصر العربية مقدمة الجلسة الثانية للجنة الخاصة (الأحكام العامة، التجريم، في مجال مكافحة استخدام تكنولوجيا الاتصالات والمعلومات لأغراض إجرامية بلورة اتفاقية دولية شاملة في إطار الأمم المتحدة] Элементы документа Арабской Республики Египет, представленного на второй сессии Специального комитета (Общие положения, криминализация, борьба с использованием ИКТ в преступных целях и разработка всеобъемлющей международной конвенции в рамках Организации Объединенных Наций)] // УНП ООН. URL: https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Second_session/Egypt_contribution_A.pdf (дата обращения: 21.04.2025).

602 Позиция была повторена и на третьей сессии. Islamic Republic of Iran (8 April 2022) // UNODC. URL: https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Second_session/Islamic_Republic_of_Iran_contribution.pdf (accessed 20.04.2025).

фундаментальное право гражданина мира) и прав человека. Отмечалось, что в современном сценарии классическая юрисдикция, основанная на Вестфальской модели, не работает в киберпространстве, особенно в отношении облачных ресурсов, что приводит к «*юрисдикционному кошмару*». В качестве примера типичной ситуации можно привести киберпреступление, совершенное с использованием вычислительных мощностей в «облаке» из одной страны, агрегации хранилищ в другом государств, при этом поставщик «облачных» услуг зарегистрирован в третьей стране, а пользователи (жертва и злоумышленник), чьи данные хранятся у поставщика услуг, может быть резидентом четвертого государства. Очевидно, что в такой ситуации крайне сложно определить юрисдикцию на основе классических территориальных моделей. Соответственно, предлагалось включить следующие любопытные пункты:

«*(e) преступление совершается с использованием компьютерных ресурсов, расположенных на территории страны;*

(f) преступление затрагивает цифровые / электронные данные их граждан, независимо от места их физического хранения / обработки / скрининга / федерализации»[603].

Иранские представители предлагали расширить существующие принципы, не выявляя новые виды: территориальный дополнить космическим объектом или спутником, зарегистрированным в соответствии с законодательством государства-участника; персональный — «преступление связано с [компьютерными данными] [электронной/цифровой информацией] граждан государства-участника, независимо от места их физического хранения, обработки или просмотра».

На сессиях Республика Индия, АРЕ и ИРИ отстаивали позицию о включении обязательства криминализации и пенализации киберпорнографии в отношении несовершеннолетних с указанием, что туда должны включаться вопросы неправомерного использования искусственного интеллекта для создания

---

[603] India (23 August 2022) // UNODC. URL: https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Second_intersessional_consultations/Revised_Indian_Text_for_UN_AHC_published_on_12.5.2022_-Revised_.pdf (accessed 20.04.2025).

соответствующего незаконного контента, а также фэйковых новостей[604]. В то время как Россия предлагала признавать уголовно-наказуемым неправомерную обработку персональных данных с использованием ИКТ, Иран — в качестве отягчающего обстоятельства в случаях, если это направлено против женщин и детей. Что касается преступлений против личности (англ. «identity-related offences»), то указанное государство поддерживало квалификацию в качестве преступлений умышленное получение или распространение паролей или учётных данных для доступа к [компьютерной системе / компьютерным данным] без права или разрешения, а равно мошенничество, недобросовестное использование электронной подписи, пароля, учетной записи, фотографии, документа или любого другого уникального идентификационного признака любого другого лица.

В рамках комитета ООН *ad hoc* был сформирована после пятой сессии группа по языковому соответствию, в состав которой входили эксперты из Доминиканской Республики, Аргентины, Беларуси, Буркина-Фасо, КНР, Кот-д'Ивуара, Эквадора, Франции, Ганы, ИХК, Казахстана, Мексики, РФ, Сингапура, Судана, Соединенного Королевства Великобритании и Северной Ирландии, США и Йемена, которые обобщали и приводили к единообразию подходы государств. Отметим частое полное или хотя бы частичное совпадение позиций КНР, Индии, Индонезии, РФ, ИРИ, АРЕ и Алжира.

В части понятийного аппарата отметим настойчивость иранского представителя указывать не только компьютерные, но и электронные системы. При этом в отличие от РФ предлагалось учитывать аппаратное (англ. «hardware») и

---

[604] См. например Islamic Republic of Iran. Reconvened concluding session of the Ad Hoc Committee (29 July to 9 August 2024, New York) // UNODC. URL: https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Reconvened_concluding_session/Written_submissions/MEMBER_STATES/Concept_note-comments-AHC.pdf (accessed 20.04.2025); Islamic Republic of Iran. Reconvened concluding session of the Ad Hoc Committee (29 July to 9 August 2024, New York) // UNODC. URL: https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Reconvened_concluding_session/Written_submissions/MEMBER_STATES/I.R.Iran-_Statement_Ad_Hoc_Committee_30_July_2024_NY.pdf (accessed 20.04.2025); Islamic Republic of Iran. Reconvened concluding session of the Ad Hoc Committee (29 July to 9 August 2024, New York) // UNODC. URL: https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Reconvened_concluding_session/Written_submissions/MEMBER_STATES/I.R.Iran-Explanation_of_Position-9_August_2024_NY.pdf (accessed 20.04.2025).

программное (англ. «software») обеспечения при определении компьютерной системы.

Ряд государств, в частности Султанат Оман[605], отмечали, что впоследствии могут потребоваться дополнительные протоколы с учётом того, насколько была сокращена Универсальная конвенция в итоговом варианте в сравнении с первоначальным и промежуточными версиями. Например, предотвращение и пресечение преступной деятельности в космическом пространстве.

Подписание конвенции государствами ожидается с осени-зимы 2025 г., а впоследствии готовится выработка дополнительных протоколов с опорой на позиции, высказанные в ходе проектирования Универсальной конвенции, а также соответствующей Конференции государств-участников через год после её вступления в силу.

С учётом проработанности стандартов контента в рассмотренных странах Глобального Юга и узконаправленности неправомерных материалов в Универсальной конвенции (фактически повторяя, а где-то и не добирая опыт Будапештской и Арабской конвенций — см. Приложение № 4) можно предположить рассмотрение вопросов, связанных не только с сексуальными надругательствами, домогательствами и интимными изображениями, но и разжиганием вражды и ненависти, деструктивными идеями, посягающих на экономическую систему государства, вероисповедания и интеллектуальную собственность, а также вовлечением несовершеннолетних в преступную деятельность и террористическими целями. Юрисдикционные принципы также могут быть расширены на основании опыта КНР, Индии и ИРИ.

Несмотря на активное участие РФ в многосторонних форматах и присоединение в качестве партнёра, наблюдается ограниченность взаимодействия. Требуется развитие двусторонних и региональных контактов за счёт создания соответствующих комиссий и межправительственных или межведомственных

---

[605] بيان وفد سلطنة عمان [Заявление делегации Султаната Оман] // УНП ООН. URL: https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Reconvened_concluding_session/Written_submissions/MEMBER_STATES/_002.pdf (дата обращения: 21.04.2025).

органов для проведения консультаций и более эффективного сотрудничества не только в рамках уголовного судопроизводства, но и по другим направлениям борьбы с преступностью. Как верно отмечается в Декларации Рио де Жанейро, подписание Универсальной конвенции «*станет эффективным инструментом и необходимой правовой основой для международного сотрудничества в целях предотвращения киберпреступности и борьбы с ней*», однако предстоит также работа по разработке дополнительных протоколов, в основу которого могут лечь высказанными государствами позиции и национальные практики в части, например, неправомерного контента[606].

§ 2. Проблемы реализации и пути совершенствования регулирования противодействия киберпреступлениям на национальном и региональном уровнях в контексте международного сотрудничества Российской Федерации и отдельных стран Глобального Юга

Международное сотрудничество включает в себя три составляющих, с позиций которых будет рассмотрены пробелы и возможности совершенствования существующей системы: правовые основы, институциональные механизмы и порядок их взаимодействия.

Прежде чем рассуждать о мерах для всестороннего и эффективного реагирования со стороны государства и общества на киберпреступления, необходимо констатировать терминологическую разобщённость в отдельных странах Глобального Юга даже в рамках традиционно выделяемых регионов: азиатском, арабском и африканском.

Хотя принцип двойной криминальности, соблюдение которого требуется при осуществлении международного сотрудничества в сфере уголовного судопроизводства, не предполагает простое совпадение наименований уголовно-

---

[606] Цыплакова А.Д. Международное сотрудничество в борьбе с киберпреступлениями: некоторые правовые проблемы в свете принятия Конвенции ООН против киберпреступности // Российский следователь. 2025. № 10. С. 62-66.

наказуемых правонарушений, лингвистические особенности всё же затрудняют первичное определение «объекта» сотрудничества и, как следствие, исследования.

При условии использования разных понятий, тем не менее, наполнение всё же может быть сходным: традиционные компьютерные преступления, которые считались частью экономических, переросли в практически любые возможные деяния с использованием ИТ в рамках конкретной системы или сети, а равно виртуального пространства в целом. Осознание невозможности криминализовать и пенализовать каждый вид киберпреступления является необходимым шагом (не сколько первым, сколь подготовительным или условно нулевым). Исходя из опыта отдельных государств Глобального Юга (в особенности арабских и африканских), внедрение широких формулировок по типу «*любое нарушение настоящего закона влечёт за собой ответственность*…», «*любое неправомерное использование технологии / в преступных целях влечёт за собой наказание*…», «*совершение [преступления] любым иным способом*…» со строго определённой санкцией позитивно способствует квалификации новых преступных посягательств без надобности принятия поправок в уголовный закон и квалифицирующих (конституирующих) признаков в виде использования ИТ / ИТС, включая сеть «Интернет» / СМИ и т.д., подобно российскому правопорядку и положениям Конвенции АС (пп. «с» п. 1 ст. 30).

Вдобавок отметим, что совершение деяний в киберпространстве может не только выступать отягчающим признаком, но и с точки зрения категории быть менее или более тяжким (в зависимости от охраняемых интересов).

Безусловно, ряд технологий по типу ИИ, Интернет вещей, Блокчейн, виртуальных активов и мета-вселенных заставляют переосмысливать традиционные категории предмета посягательства (имущества, валюты) и даже субъекта ответственности. Определение места совершения преступления (в том числе цифрового) особенно актуально для изучения с точки зрения установления уголовной юрисдикции и, как следствие, для защиты суверенных интересов государства. Хотя возможно оставить попытки переиначивания и адаптации, изменения в законодательствах других государств неумолимо требуют

своевременной реакции и российских законодателей и правоприменителей для эффективного международного сотрудничества. На сегодняшний день в виртуальном пространстве государственные границы размываются. Возможен учёт опыта Республики Индия (юрисдикция, основанная на гражданстве лица, которому принадлежат данные, а не территории их хранения, обработки, скрининга или федерализации, территориальное расположение использованных при совершении преступления компьютерных ресурсов), Исламской Республики Иран (домен верхнего уровня веб-сайта с кодом страны Ирана «.ir» как юрисдикционная привязка), КНР, АНДР (направленность посягательства на государственные институты, национальную оборону или стратегические интересы национальной экономики[607]) как при разработке протокола к Универсальной конвенции и других соглашений, так и при совершенствовании национальных уголовных законов. Интересен и опыт приоритетности юрисдикционных привязок Арабской конвенции, который разрешает коллизию первого порядка. В зависимости от вида преступлений может отдаваться предпочтение разным юрисдикционным принципам для защиты суверенных интересов: в случае посягательства на данные лица приоритет может отдаваться исходя из гражданства потерпевшего; при ущербе компьютерным системам (устройствам) — их принадлежности (организации или государству; при ущербе Интернет-ресурсам — принадлежности доменов как примеры расширения персональных и защитного принципов. С точки зрения осуществления МССУС — наиболее тесная публично-правовая связь с преступником. Привязка к территориальности расположения использованных ресурсов или хранения, обработки, скрининга или федерализации данных имеет практическую применимость скорее к процессуальной правоприменительной юрисдикции.

С учётом разнородности и неустойчивости избранного понятийного аппарата, в котором и проявляется возможное многообразие, отметим разный уровень подготовленности и оснащённости государств Глобального Юга. Он может

[607] Хотя он и корреспондирует традиционному защитному принципу, специфика проявляется в терминологии и уточнениях применимости в отношении именно киберпреступлений.

оцениваться и совершенствоваться, исходя из трёх позиций: технические и человеческие ресурсы, организационные меры (мероприятия) и регулирование. Рассмотренные «разношёрстные» проблемы демонстрируют необходимость равнозначного и равномерного развития каждого из перечисленных элементов.

Отсутствие чёткой нормативно-правовой базы для внедрения технологий во благо отдельных экономических процессов, государства, да и общества в целом сопровождается порождением новых пробелов и лазеек для совершения новых уголовно наказуемых деяний[608], что впоследствии затрудняет и международное сотрудничество. Цифровые двойники граждан, инфраструктуры и целых городов[609], а также «валют» как новое выражение субъекта, предмета посягательства (средства) и места совершения преступления не предусмотрены действующими уголовными и уголовно-процессуальными законами. На доктринальном уровне ведётся научный дискурс и активным образом изучается возможность перенесения в виртуальный мир. Необходима выработка универсального (единообразного) подхода к цифровым двойникам: признание и уравнивание в статусе либо выработка специального режима. Полное же игнорирование, очевидно, оставляет граждан без судебной защиты своих интересов. Даже расширительное толкование требует законодательных разъяснений (судебного толкования [610]) или соответствующего закрепления и не может базироваться на умозрительном теоретизировании. Хотя российская юридическая техника не подразумевает использования обозначенных выше формулировок, они распространены в зарубежных странах и отдельных международных договорах, что необходимо учитывать как при формировании уголовной политики[611], так и при осуществлении

---

[608] А порой ещё пока не наказуемых по уголовному закону, но очевидно посягающих на охраняемые законом интересы.

[609] В перспективе обсуждается вопрос и целого государства в метавселенной.

[610] В зависимости от принятой правовой традиции в государстве.

[611] Как одно из направлений правовой политики (в частности) и государственной политики (в целом), она выражается в разработке мер уголовно-правового и уголовно-процессуального воздействия и обеспечивающих их мер финансового, гражданского и информационного права. См. подробнее Долгиева М. М. Теоретические основания уголовной политики в сфере оборота криптовалюты: диссертация на соискание ученой степени доктора юридических наук / Долгиева Мадина Муссаевна. Москва, 2023. 474 с. С. 54.

сотрудничества. Полисемичность таких терминов, как «цифровой объект преступления», «цифровой ущерб от преступления», «цифровое место преступления», конечно же, требует обоснования[612]. Тем не менее это уже скорее данность для ряда стран, в частности арабских и КНР.

С точки зрения институциональных механизмов отметим следующее: неформальные контакты и каналы ограничиваются обменом оперативной информацией и опытом, однако для полноценного взаимодействия требуются более формализованные контакты и корреспондирующая правовая основа. На многостороннем уровне при открытости странам Глобального Юга, которые являются дружественными, наблюдаются ограничения из-за статуса РФ и невозможности присоединения к ряду региональных организаций. Несмотря на активное расширение БРИКС в части как партнёров, так и членов объединения, наблюдается практика регламентации и взаимодействия не по уголовно-правовым и уголовно-процессуальным вопросам. Вдобавок, даже будучи в составе ряда организаций и объединений, государства Глобального Юга не спешат присоединяться к разработанным международным договорам. Соответственно скорее приемлем формат двустороннего уровня, на котором учреждаются совместных комитетов (комиссий) по борьбе с преступностью (отдельными видами преступлений). Они, в свою очередь, могут способствовать более эффективному межгосударственному взаимодействию.

Исходя из отечественной правовой мысли[613], противодействие включает в себя деятельность органов государственной власти, физических и юридических лиц:

---

[612] Долгиева М. М. Цифровой объект преступления // Вестник Томского государственного университета. 2022. № 483. С. 253-260; Долгиева, М. М. Цифровой ущерб от преступления: практические вопросы // Вестник Томского государственного университета. 2023. № 487. С. 206-211.

[613] В то время как в научном дискурсе уже много лет (веков) нет единой или хотя бы единообразной позиции, целесообразно сосредоточиться на законодательном подходе, а также международных договорах. См. подробнее Федеральный закон от 6 марта 2006 г. № 35-ФЗ «О противодействии терроризму» // Собрание законодательства Российской Федерации. 2006. № 11. Ст. 1146; Федеральный закон от 25 декабря 2008 г. № 273-ФЗ «О противодействии коррупции» // Собрание законодательства Российской Федерации. 2008. № 52 (часть I). Ст. 6228;

1) по предупреждению преступлений, в том числе по выявлению и последующему устранению причин и условий, способствующих совершению преступлений (*профилактика*);

2) по выявлению, предупреждению, пресечению, раскрытию и расследованию правонарушений (*борьба*);

3) по минимизации и (или) ликвидации последствий правонарушений и проявлений радикализма;

4) по осуществлению международного сотрудничества[614].

Первому и третьему направлениям корреспондирует криминологическая часть исследования (глава II), второму — уголовно-процессуальная (глава III), четвертому — глава IV.

Многообразие совершаемых и потенциальных киберпреступлений не позволяет составить единый портрет личности преступника[615], выявить единые причины и условия и, следовательно, одинаковые меры реагирования. Тем не менее предупреждение, нередко включающее в себя профилактику, базируется на руководящих и организационных документах, необязательно носящих нормативный характер, иногда разработанных во взаимодействии с деятелями науки и правоприменителями. Стратегии рассмотренных государств сосредоточены на развитии управления (нормативно-правовой базы, стандартов, технической защищённости инфраструктуры и механизмов реагирования на инциденты) с опорой на риск-ориентированный подход в отдельных случаях, (вертикального и горизонтального / внутригосударственного и внешнего) сотрудничества, наращивании кадрового потенциала и финансировании НИОКР, повышение грамотности, культуры и доверия у населения, цифровой

Федеральный закон от 25 июля 2002 г. № 114-ФЗ «О противодействии экстремистской деятельности» // Собрание законодательства Российской Федерации. 2002. № 30. Ст. 3031.

[614] Tsyplakova A.D. Forms of Impact on Crime and their Significance. II International Scientific and Practical Conference ‘Strategies for Countering Crime in a Changing Reality’. Sevastopol: the Law Institute of Sevastopol State University, 22 May of 2025. URL: http://dx.doi.org/10.2139/ssrn.5248584.

[615] Искусственно созданное, обобщающее криминологическое понятие для характеристики присущих физиолого-психологических свойств, особенностей экономического и социального положения индивида, совершающего преступление.

трансформации отдельных секторов и государства в целом. Вследствие столь широкой повестки практически все государственные органы и многие представители частного сектора задействованы прямо или косвенно в сфере кибербезопасности, становясь субъектами или объектами воздействия. Инициативы затрагивают не только обучение, но и выработку новых методик расследования и систем реагирования, включая интеграцию искусственного интеллекта и электронного документооборота.

Проблемы должны рассматриваться не изолированно друг от друга, а в комплексе: наряду с своевременной криминализацией и пенализацией новых форм преступного использования ИКТ повышать квалификацию кадрового состава государственных (не только правоохранительных) органов, просвещать население через соответствующих амбассадоров и киберволонтёров в форме, доступной для различных уязвимых групп населения, формировать защищённые платформы с назначением ответственных для межведомственного взаимодействия, оперативной передачи информации и избежания дублирования (и, как следствие, бюрократического затягивания), а также расширять учёты и доступы правоохранительных органов к существующим АСОД (ИС) в государстве.

Борьба с киберпреступлениями подразумевает уголовное преследование и сопровождающие его процессуальные меры. Для привлечения лиц к ответственности не только за киберпреступления, но и за традиционные виды деяний, закрепление криминалистически важной информации в электронной форме имеет особое значение. Исходя из проведённого анализа, можно констатировать, что признание цифровых доказательств в качестве отдельного вида или подвида доказательств в рамках именно уголовного процесса стало «стандартом» как для стран Глобального Юга, так и на международном уровне (подтверждением чего служит Универсальная конвенция, устанавливающая обязательство сотрудничать по вопросам доказательств *в электронной форме*[616]).

---

[616] Терминологически ближе к индийскому и китайскому (САР Макао) подходам, но не по содержанию, оставляя на усмотрение государств-участников трактование.

Вместе с тем в Российской Федерации, несмотря на давнюю полемику[617], до сих пор нет единого понятийно-категориального аппарата, в том числе легального определения, а также статуса у электронной информации именно как доказательства, что ограничивает субъектов уголовного преследования ввиду необходимости привязки к конкретной форме, которая не всегда корреспондирует материальному миру: оформление протоколом осмотра предметов (документов) осмотр сети «Интернет» представляется нелогичным, но тем не менее почти единственным способом процессуального закрепления цифровых следов, помимо соответствующей экспертизы и иных документов (в части приобщения ответов юридических лиц, которым принадлежат социальные сети или которые оказывают Интернет-услуги). Вместе с тем именно такой узкий и порой пробельный подход не позволяет в полной мере реализовать возможный потенциал для эффективной и быстрой ВПП по УД и оперативного обмена информацией, в том числе при разработке соответствующих банков цифровых следов.

С этим сопряжено и немало рисков, особенно в контексте введения электронного документооборота: достоверность цифровых доказательств, порядок ознакомления с ними в системе ЭДО, обеспечение конфиденциальности и т.н.

---

[617] См., например: Васюков В.Ф., Булыжкин А.В. Изъятие электронных носителей информации при расследовании преступлений: нерешенные проблемы правового регулирования и правоприменения // Российский следователь. 2016. № 6. С. 5; Агибалов В.Ю. Виртуальные следы в криминалистике и уголовном процессе: автореф. дис. ... канд. юрид. наук. Воронеж: Воронежский государственный университет, 2010. С. 13; Сукманов А. О. Сущность, понятие и виды электронно-цифровых следов, используемых в раскрытии и расследовании преступлений // Вестник Калининградского юридического института МВД России. 2010. № 4 (22). С. 104-107; Колычева А.Н. Фиксация доказательственной информации, хранящейся на ресурсах сети Интернет: автореф. канд. юрид. наук. М., 2019. С. 25; Вехов В.Б., Смагоринский Б.П., Ковалев С.А. Электронные следы в системе криминалистики // Судебная экспертиза. № 2. С. 17; Россинская Е.Р., Семикаленова А.И. Основы учения о криминалистическом исследовании компьютерных средств и систем как часть теории информационно-компьютерного обеспечения криминалистической деятельности // Вестник Санкт-Петербургского университета. Право. 2020. № 11(3). С. 752; Себякин А.Г. Тактика использования знаний в области компьютерной техники: монография. М.: Юрлитинформ, 2023. С. 24; Антонов О. Ю. Анализ цифровой информации как одна из задач криминалистического исследования компьютерных средств и систем // Вестник криминалистики. 2020. № 2 (74). С. 17-23; Поляков И. С. Понятие, классификация электронных следов и их криминалистическое значение // Вестник Академии Следственного комитета Российской Федерации. 2024. № 4 (42). С. 169-176; Поляков И.С. Особенности элементов механизма образования электронных следов в сети Интернет // Сибирские уголовно-процессуальные и криминалистические чтения. 2025. № 2. С. 70–81.

«тайны расследования», а также межгосударственное взаимодействие фактически посредством незащищённых каналов связи (электронные почтовые ящики). Как показывает практика, в ряде случаев это предполагается решить с помощью Блокчейна.

Также в качестве проблемы можно выделить разницу в сроках хранения данных поставщиками услуг и действия приказов об их сохранении, которая зачастую относится к усмотрению конкретного государства, поэтому на международном уровне может быть (предположительно) выработан лишь минимальный уровень или критерий.

В то время как вопросам правового статуса и процессуального оформления электронных доказательств уделено (относительно) достаточное внимание в рассмотренных зарубежных странах, регламентация проблемного контента, порядка его блокировки недостаточна в ряде стран Глобального Юга и не раскрыта на международном уровне: ни в Будапештской, ни в Арабской, ни в Универсальной конвенциях, ни в Соглашении ШОС, ни в Конвенции АС нет соответствующих положений. Корреспондирующие нормы, определяющие контент неправомерным не только в части порнографических материалов, но и противоречащих интересам государств, также могут стать предметом дополнительного протокола в рамках как универсального и региональных, так и двусторонних международных договоров. В качестве образца могут быть взяты отдельные арабские и азиатские страны. Важно, чтобы, помимо того, что блокировка Интернет-ресурсов, содержащих запрещённые сведения[618], осуществлялась через т.н. «чёрный список» Роскомнадзора, партнёры были надлежаще извещены и ограничивали доступ к ним, обеспечивая всестороннее пресечение уголовных правонарушений на собственной территории, особенно с учётом использования средств обхода блокировок — VPN и TOR.

[618] Фактически вносятся IP-адрес, доменное имя веб-сайта или адрес конкретной страницы. В первом случае логика заключается в том, что IP-адреса могут принадлежать адресному пространству РФ, следовательно, теряются арендуемые вычислительные мощности у преступников. Во втором — российские Интернет-провайдеры не обрабатывают запросы к конкретному DNS-серверу.

При этом одной из проблем является отсутствие регламентации порядка взаимодействия следственных органов и провайдеров Интернет-услуг, агрегаторов (связи), в особенности с иностранными [619] . При воспрепятствовании осуществлению правосудия: подлоге или сокрытии доказательств, в том числе цифровых, введении в заблуждение следствия или суда, непредоставление документов — общеуголовными законами отдельных государств предусмотрена ответственность. В то время как в практике стран Глобального Юга не возникает проблем при направлении соответствующих запросов зарубежным юридическим лицам, для Российской Федерации данный вопрос стоит особо остро. Вероятно, глобальные или региональные криминалистические учёты и т.н. банки цифровых следов (информационные системы обмена электронной информацией [620]) могут расшириться до данных, предусмотренных Универсальной конвенцией, и способствовать эффективному и быстрому обмену информацией, необходимой для расследования киберпреступлений. Вдобавок проработка вопроса о возможной

---

[619] Скобелин С. Ю. Сложные вопросы расследования киберпреступлений // Советская и российская криминалистика: традиции и современные векторы: Материалы всероссийской научно-практической конференции, Москва, 29 февраля 2024 года. Москва: Московская академия Следственного комитета им. А.Я. Сухарева, 2024. С. 228-231.

[620] Безусловно, для начала необходимо иметь на национальном уровне «*криминалистическую систему, позволяющую идентифицировать пользователей сети Интернет по электронно-цифровым следам*» и содержащую объекты, «*необходимые для расследования киберпреступлений, особенно носящих организованный преступный характер*», к которой имели бы доступ все правоохранительные органы, а также межведомственную сеть. См. об этом подробнее Бастрыкин А. И. Выявление и расследование преступлений, совершенных с использованием информационно-коммуникационных технологий // Вестник Российской правовой академии. 2022. № 4. С. 88-94; Бессонов А. А. О некоторых направлениях совершенствования криминалистического обеспечения расследования киберпреступлений // Расследование преступлений: проблемы и пути их решения. 2024. № 2(44). С. 31-37.
О реализации идеи информационной системы обмена электронной информацией идёт речь в рамках СНГ, тем не менее её можно было бы расширить до иных существующих институциональных механизмов международного полицейского сотрудничества. См. подробнее Заместитель Генерального секретаря СНГ Н. Сейтимов принял участие в заседании Совета руководителей органов безопасности и специальных служб государств – участников СНГ // Интернет-портал СНГ. Пространство интеграции. 16.05.2025. URL: https://e-cis.info/news/564/127418/ (дата обращения: 10.06.2025); Волеводз А.Г., Цыплакова А.Д. Международное полицейское сотрудничество: современная институциональная структура и тенденции развития // Международное уголовное право и международная юстиция. 2023. № 3. С. 2-6.

трансграничной передаче данных [621] в целях именно международного сотрудничества в борьбе с преступностью (в целом) или в сфере уголовного судопроизводства (в частности) должна находить своё отражение в соответствующих дву- и многосторонних международных договорах (или протоколах к ним).

С точки зрения как предмета посягательства, так и наложения обеспечительных мер отметим, что в Универсальной конвенции и законодательстве ряда государств Глобального Юга под имуществом для уголовно-процессуальных, гражданско-процессуальных и антиотмывочных целей понимаются в том числе виртуальные активы, которые могут охватывать не только т.н. криптовалюту, но и иные цифровые «сущности» по типу NFT ввиду достаточно широких дефиниций довольно давно. При этом порядок общий и довольно типичный без учёта технических особенностей. Примечательно, что не наблюдается регламентации порядка хранения и реализации конфискованных виртуальных активов. Хотя есть отдельно сложившаяся негласная практика в КНР: продажу местными органами через частные компании. Также предполагается использование специальных административных районов с отличительным регулированием[622]. САР в сравнении с СЭЗ, где обычно действует общее уголовное (материальное и процессуальное) право, имеет особенности и порой всецело отдельное (иногда противоположное) регулирование, хотя у последних также есть специфика с позиции компетентных органов. Подобные пробелы и исключения в целом могут осложнить последующий возврат преступных активов из-за рубежа и/или их раздел. Вместе с тем имеются и механизмы для ускорения производства отдельных процессуальных действий в

[621] В Универсальной конвенции идёт речь о персональных данных (данных об определяемом или определённом физическом лице) и оговорке о необходимости получения разрешения в возможном письменном виде.

[622] China debates how to handle criminal crypto cache // Reuters. 17.04.2025. URL: https://www.reuters.com/world/china/china-debates-how-handle-criminal-crypto-cache-2025-04-15/ (accessed 22.05.2025); China to Liquidate Seized Cryptocurrency Through Licensed Hong Kong Exchanges // Coinfea. 07.06.2025. URL: https://www.binance.com/en/square/post/25293712456530 (accessed 07.06.2025).

части осуществления ВПП по УД[623] (особенно с привлечением т.н. инспекторов и иных лиц, наделённых статусом *мамурийя ад-добты аль-кодоийи*, в арабских странах теоретически возможен, хотя и сложен).

В Российской Федерации же, помимо терминологических особенностей (*цифровая* валюта, не являющаяся средством платежа, *цифровой* рубль как третье выражение законного средства платежа и электронные средства платежа), долгое время наблюдалась оторванность отраслей законодательства друг от друга. Хотя с учётом недавно разработанных поправок в отечественные уголовный и уголовно-процессуальный законы[624] можно отметить частичное восполнение пробелов: не учтены, например, горячие кошельки, цифровые финансовые активы. Предстоит разработка порядка хранения изъятого «цифрового» имущества. При этом в зарубежных странах подробной регламентации подобного не обнаружено, хотя на практике и зафиксированы соответствующие случаи[625].

Вероятно, в случае подписания Универсальной конвенции будут вноситься соответствующие поправки в действующее регулирование стран, поскольку она содержит прогрессивные[626] положения о конфискации без приговора, возврате преступных доходов[627], доказательствах в электронной форме[628] и имуществе (включая виртуальные активы). Вместе с тем могут разрабатываться дополнительные протоколы для того, чтобы служить комплексной правовой

---

[623] Обычно именно этот вид запроса корреспондирует, хотя в отдельных странах по типу Индонезия исполнение запросов о конфискации выделяется в отдельное направление (подвид).

[624] Законопроект № 902782-8. О внесении изменений в статью 104-1 Уголовного кодекса Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации (об особенностях изъятия цифровой валюты) // Система обеспечения законодательной деятельности. URL: https://sozd.duma.gov.ru/bill/902782-8 (дата обращения: 20.06.2025).

[625] См. Клевцов К.К., Цыплакова А.Д. Противодействие криптовалютным преступлениям в некоторых странах смешанных правовых систем // Противодействие криптовалютным преступлениям в зарубежных странах. М.: ООО Издательский дом «Юрлитинформ», 2025. С. 399-402; Цыплакова А. Д. Противодействие криптовалютным преступлениям в странах Среднего и Ближнего Востока и Северной Африки // Противодействие криптовалютным преступлениям в зарубежных странах. М.: ООО Издательский дом «Юрлитинформ», 2025. С. 402-490; Singh V.V. 6,600 crore bitcoin scam: ED seizes 1.6 crore Dubai assets // The Times of India. 20.02.2025. URL: http://timesofindia.indiatimes.com/articleshow/118395033.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst (accessed 03.06.2025).

[626] Для отдельных стран по типу Индонезия и Индия.

[627] Однако без положений об их разделе.

[628] Особо актуально для РФ.

основой международного сотрудничества для Российской Федерации и отдельных стран Глобального Юга[629].

Таким образом, существующие проблемы регулирования противодействия киберпреступлениям как комплексного явления связаны с разным уровнем технологического развития, правовой культурой и традициями стран Глобального Юга. При всей «южной солидарности» разрыв в инфраструктуре и ресурсах весьма ощутим и сообразно отражается на внутригосударственном и межгосударственном уровнях. С правовой точки зрения констатируем каузальность отдельных норм, не адаптированных к постоянно меняющейся реальности фундаментальных категорий, начиная от криминализации и пенализации и заканчивая воздействием на киберпреступность, причём действующая и будущая международно-правовая база не в полной мере соответствует вызовам и угрозам на фоне уже не первого десятка лет длящегося генезиса. Универсальная конвенция как предположительно наиболее совершенный документ является результатом консенсуса полярных мнений стран Глобального Севера и Глобального Юга и, как следствие, не лишен недостатков. Хотя в ней закреплен правовой статус электронной информации как доказательства, не учтены положения о преступном использовании отдельных достижений пятой революции, новые (возможные) виды юрисдикционных привязок, предлагавшиеся азиатскими странами, а также понятие деструктивного (запрещённого) контента и порядок его блокировки (ограничения доступа к нему). Именно национальный опыт может быть положен в основу изменений, хотя не следует злоупотреблять чрезмерной регламентацией.

Институционально же проблематика международного сотрудничества состоит в ограниченности взаимодействия: невозможность присоединения к отдельным организациям и объединениям и (или) нежелание формализовывать уголовно-правовые вопросы. В подобном случае остаются двусторонние контакты, которые требуют более активного развития в контексте комитетов (комиссий), из

---

[629] Цыплакова А.Д. Международное сотрудничество в борьбе с киберпреступлениями: некоторые правовые проблемы в свете принятия Конвенции ООН против киберпреступности // Российский следователь. 2025. № 10. С. 62-66.

чего прямо вытекают и сложности порядка непосредственного взаимодействия: начиная от разницы в понимании рассматриваемого феномена и заканчивая применением традиционных механизмов к *кибер*-составляющей.

ЗАКЛЮЧЕНИЕ

В настоящем исследовании, исходя из поставленной цели и вытекающих из нее задач, обозначены и проанализированы основные направления противодействия киберпреступлениям в отдельных странах Глобального Юга, которые отражают основные тенденции: криминализация и пенализация, правовые основы, институциональные механизмы, порядок их взаимодействия, отдельные профилактические инициативы, особенности уголовного преследования и межгосударственного взаимодействия в борьбе с преступностью. Исследованы нормативные правовые базы арабских стран, в частности Аравийской зоны (Объединённых Арабских Эмиратов, Королевства Саудовская Аравия, Государства Катар, Султаната Оман, Королевства Бахрейн, Государства Кувейт), аль-Машрика (Иорданского Хашимитского Королевства), аль-Магриба (Арабской Республики Египта, Алжирской Народной Демократической Республики, Тунисской Республики, Королевства Марокко), Африки (Федеративной Демократической Республики Эфиопия), Азии (Исламской Республики Иран, Республик Индия и Индонезия, Китайской Народной Республики) с учётом специфики иностранных языков (арабского, персидского, китайского, индонезийского, французского, английского, амхарского, португальского), принадлежности правовых систем, источников права (законодательства), вертикального и горизонтального уровней (внутри государств и между ними).

С точки зрения уголовно-правового содержания определено, что отсутствует единая позиция при обозначении, определении и охвате уголовно-наказуемых деяний. В узком смысле киберпреступления охватывали (экономические) компьютерные преступления, что корреспондировало первоначальному законодательному и правоприменительному подходам. Основным признаком определения кибердеяний является формальный признак. С учётом юрислингвистических особенностей и юридической техники построения законов (см. Приложения №№ 1–3) в самом широком смысле киберпреступления подразумевают использование ИКТ (современных технологий) в преступных целях, в том числе посягательства на данные, информационные (компьютерные) сети,

системы, устройства (в т.ч. АСОД и автоматизированные информационные системы), личность (честь и её достоинство), цифровые объекты (документы идентификации, в том числе подписи, печати и сертификаты, электронные средства платежа и виртуальные активы, электронные документы), права интеллектуальной собственности, интересы потребителей, охраняемые законом тайны, правонарушения регулирования телекоммуникационного сектора, оказания сертифицированных услуг, правила пользования социальными сетями, мессенджерами, средствами связи и публикаций, в том числе электронной рекламы и контента, ЭДО в государственном и частном секторах, обеспечения безопасности объектов критической (информационной) инфраструктуры, удалённой работы, оказания государственных услуг, электронного голосования, электронной торговли и юридической деятельности. Особую группу составляют правонарушения лицензируемой деятельности. Тем не менее существующим киберрегулированием не запрещены мета-преступления, цифровые наркотики, электронные мухи, посягательства на внутриигровые активы, исходя из складывающейся типологии киберпреступлений.

Киберпреступления могут быть классифицированы, исходя из легального, законодательного, доктринального подходов, этики использования и стандартов медиаконтента, а также делиться на кибер-зависимые деяния (англ. «cyber-dependent crimes») и деяния с кибервозможностями (англ. «cyber-enabled crimes»).

Для соблюдения принципа двойной криминальности необходимо учитывать, подписантами каких международных договоров являются отдельные страны Глобального Юга и какова степень имплементации разнящихся документов (см. Приложение № 4), а также учитывать неуголовно-правовое и процессуальное регулирование при установлении преступности и наказуемости (см. Приложение № 2) и разницу в элементах состава преступления. Отметим сочетание начал уголовной и административной ответственности в зарубежных странах, что влияет на круг наказаний и компетентных органов по их назначению. Субъектами выступают как физические, так и юридические лица. При совершении

киберпреступлений могут назначаться общеуголовные и специфические наказания (но без цифровой составляющей).

Международные договоры, равно как и национальное законодательство, оказали друг на друга взаимопроникающее влияние. Вдобавок сложившиеся правовые традиции в рамках конкретной правовой системы, принадлежность которой не всегда однозначна, равно как и особенности юридической техники, находят своё проявление в общих правилах построения норм и квалификации деяний как составляющей правоприменения (установлении всех элементов составов преступлений, количество которых также может разниться).

Хронологически (в особенности в 2010-е гг.) параллельно развитию уголовных и уголовно-процессуальных законов принимаются стратегии, руководства и концепции скорее уполномоченными органами, нежели высшими должностными лицами. Оба прошли долгий путь становления, расширяясь с точки зрения наполнения и статуса. Стратегии (см. Приложение № 5) обновляются примерно раз в 5–7 (5–10) лет и охватывают не только кибербезопасность, но и смежные области: данные (их защита и конфиденциальность), ИИ, электронные коммуникации, транзакции, подписи, правительство, предоставление государственных услуг, цифровые трансформация, экономика (электронная коммерция, ЭСП), аутентификация, Интернет вещей, автоматизация процессов, Блокчейн, ЭДО, умные города, защита потребителей и интеллектуальной собственности. Отражая основные тенденции, стратегии при этом не касаются отдельных достижений, например квантовых технологий. Стандартизация охватывает не только КИИ, контент в сети «Интернет», но и его технические составляющие, а также управление кадровыми ресурсами, физическими мощностями (пример см. Приложения №№ 6, 7). Сферами деятельности выступают выявление талантов, укрепление этического использования ИТ, повышения киберосознанности и кибергигиены населения, а также международное сотрудничество и государственно-частное партнёрство.

Несмотря на превалирующую позицию в исключительной компетенции государства (федерации / республики) по уголовному и уголовно-процессуальному

праву, выявлено регулирование на уровне ОЭЗ (СФЗ), САР и субъектов, которое может быть отличным либо более широким в сравнении с обозначенным выше. Это в свою очередь позволяет не только экономически развивать государство, но и оперативно реагировать на отдельные вызовы и угрозы цифровой эпохи. Помимо руководящих документов, специфичных для конкретных территорий, культур и секторов, обнаружены органы, которые могут участвовать в уголовном преследовании: фиксировать правонарушения, собирать криминалистически значимую информацию, производить первоначальные следственные действия, участвовать в наложении обеспечительных (т.н. антиотмывочных) мер, проведении экспертиз и выступать в качестве специалистов. Задействование представителей органов исполнительной власти не является новшеством для стран Глобального Юга, в особенности арабских и африканских, однако оно может быть учтено в отечественном регулировании и правоприменении.

В отдельную группу криминологической составляющей противодействия киберпреступлениям можно выделить белые книги, составляемые представителями теории и практики, (не)государственные органы, организации и лица, которые выступают вспоминающими при расследовании инцидентов и преступлений. Задействованные в сфере кибербезопасности органы выполняют нормативную, координирующую, научно-исследовательскую, просветительскую, правоохранительную и связующую функции, одновременно совмещая, разделяя или делегируя их. Реализуемые инициативы можно поделить на профилактические (просветительские), экономико-технические (развитие государственно-частного партнёрства) и пресекательные (развитие систем реагирования и баз данных).

На региональном уровне документы по борьбе с преступностью в целом и киберпреступностью в частности датируются 2000-ми годами в азиатском регионе, 2010-ми — в арабском, 2020-ми — в африканском. Фактически они либо носят общий стратегический характер, либо напрямую не касаются уголовно-правовых и уголовно-процессуальных вопросов. Специализированные органы включают в себя министерские встречи, рабочие группы, исполнительные комитеты и CERT. Самый большой аппарат обнаружен в рамках АСЕАН (среди рассмотренных); ЛАГ,

ССАГПЗ и БРИКС уступают по численности. Африканские объединения и организации находятся в начале пути их становления.

Уголовное преследование за киберпреступления сопряжено с признанием доказательств в электронной форме и их процессуальным оформлением, использованием передовых технологий (ЭДО, ИИ, Блокчейн, 3D-симуляции, ИС / АСОД, видеоконференцсвязь), ограничением доступа или изъятием неправомерного контента, мерами процессуального принуждения (в т.ч. электронного мониторинга), трансграничной передачей данных, а также наложением обеспечительных мер на виртуальные активы и осуществлением МССУС. Даже при условии отсутствия легального статуса цифровых доказательств в некоторых странах Глобального Юга (в ретроспективе[630] и/или в настоящее время[631]) сложилась устойчивая судебная практика по принятию таковых при условии соблюдения минимальных требований и принципов. Механизм по обыску, сохранению и последующему изъятию данных (устройств) либо по входу/доступу разнится: судебный, внесудебный и смешанный. Ряд действий возможен без судебного решения (e.g., перехват в ФДРЭ и Тунисе, выемка и контроль электронных сообщений в арабских странах). Отличаются и сроки хранения данных провайдерами услуг, в зависимости от типа и станы: в Катаре информация о пользователях — в течение 1 года; данные о ИТ — не менее 120 дней; временное и срочное хранение данных информационных технологий, данных о трафике или контент — в течение 90 дней; АНДР и ФДРЭ — 1 год; Иран — не менее 15 дней трафик и не менее 6 месяцев хостинг-услуги. Возможно, стоило бы установить единые международные стандарты в этой части для более оперативного обмена информацией.

Выявлены полисематичность ряда понятий, в частности цифровых (виртуальных) имущества, места преступления (происшествия), объекта, что уже скорее данность для стран Глобального Юга в антиотмывочных целях и для эффективного противодействия, а также расширительное толкование

---

[630] СО, КСА, ОАЭ, ФДРЭ, ИХК, КНР, Республика Индия.
[631] Тунисская Республика, АНДР, Королевство Марокко.

формулировок и применимость гражданско-правовых и гражданско-процессуальных норм в качестве *lex specialis*.

Содержание неправомерного контента, порядок его удаления или ограничения доступа к Интернет-ресурсам является острой проблемой для стран Глобального Юга, при этом регламентация указанных вопросов носит фрагментарный характер и в отдельных случаях оставлено на усмотрение правоприменителей. Тем не менее они представляются важными в контексте всестороннего противодействия киберпреступлениям и осуществления международного сотрудничества.

Основной проблемой при реализации международного сотрудничества в борьбе с преступностью в целом и уголовном судопроизводстве в частности является ограниченность существующих институциональных механизмов (ЛАГ, ОИС, ССАГПЗ, АС, IGAD и АСЕАН), неприсоединение ряда государств к международным договорам (например, в рамках ШОС) или их отсутствие (БРИКС). Активно развивается практика двусторонних форматов в виде совместных комитетов и комиссий в зарубежных странах, возможна проработка расширенных криминалистических учётов (банков электронных / цифровых следов) в рамках, например, международных полицейских организаций.

Несмотря на принятие Универсальной конвенции, её нельзя считать «панацеей» с учётом противоположных позиций стран Глобального Юга и Глобального Севера при выработке консенсуса. Предстоит большая работа по выработке дополнительных протоколов в части возможных обязательств по криминализации и пенализации призывов к мятежу, оскорблению религий, стран, государственной символики, посягательств, разжигающих вражду или ненависть, уголовно-правового запрета на использование ИКТ при нападениях на гражданские объекты и ИИ, а также понятия неправомерного контента, порядка ограничения доступа к нему и новых юрисдикционных принципов. Тем не менее положения Универсальной конвенции может восполнить пробелы, например, в части правового статуса электронных доказательств и виртуальных активов в

отечественном регулировании; в части наложения обеспечительных мер, в том числе конфискации без приговора, — в Республиках Индия, Индонезия и Иран.

Появление цифровых двойников требует комплексного подхода не только к основной, но и смежным проблемам. Внедрение какой-либо технологии по типу ИИ и Блокчейн сопряжено и с рисками, которые необходимо учитывать при переходе от интроверсии к сдерживающей или умеренной экстраверсии.

Для целей международного сотрудничества в сфере борьбы с преступностью представляется целесообразным:

1) использовать более универсальные конструкции составов киберпреступлений в отечественном регулировании;

2) уточнить однозначно правовой статус цифровых (электронных) доказательств и порядок их получения, а также положение виртуальных активов и их видов, порядок наложения ограничительных мер на них в российском законодательстве;

3) рассмотреть возможность внедрения таких инициатив, как киберволонтёры и/или электронные амбассадоры, базы данных открытого и закрытого типа с подозрительными абонентскими номерами, электронными почтовыми ящиками в целях противодействия кибермошенничеству, единые системы автоматизированного реагирования на инциденты и подозрительные операции в критически важных сферах и использование возможностей ИИ для криминалистического обеспечения расследований, в России;

4) выработать единообразное понятие противоправного контента и установить минимальные сроки хранения данных, а также обеспечить сотрудничество в сфере блокировки и/или ограничения доступа к противоправному контенту и/или Интернет-ресурсам, содержащих его, путём разработки и принятия соответствующего Дополнительного протокола к Универсальной конвенции (с учётом опыта стран Глобального Юга);

5) создавать защищённые глобальные банки электронных следов и развивать двусторонние контакты посредством учреждения межгосударственных (межведомственных) комитетов (комиссий) в борьбе с преступностью.

СПИСОК ИСПОЛЬЗОВАННЫХ СОКРАЩЕНИЙ

Сокращения

АНДР — Алжирская Народная Демократическая Республика.

Арабская конвенция — Арабская конвенция о борьбе с преступлениями в области информационных технологий (Каир, 21.12.2010).

АРЕ — Арабская Республика Египет.

АС — Африканский союз.

АСЕАН — Ассоциацию государств Юго-Восточной Азии.

АСОД — автоматизированная (-ые) система (-ы) обработки данных.

Будапештская конвенция — Конвенция о киберпреступности (Будапешт, 23.11.2001).

АТР — Азиатско-тихоокеанский регион.

АТЭС — Азиатско-Тихоокеанское экономическое сотрудничество.

БТС — беспилотное транспортное средство.

ВПП по УД — взаимная правовая помощь по уголовным делам.

ВС — Верховный суд.

Дахир № 1-20-69 — указ короля Марокко № 1-20-69 от 25.06.2020 «О принятии закона № 05-20 «О кибербезопасности».

Декларация Рио-де-Жанейро — Декларация «Укрепление сотрудничества Глобального Юга для более инклюзивного и устойчивого управления» (Рио-де-Жанейро, ФРБ, 06.07.2025).

ЕС — Европейский союз.

Закон Бахрейна № 60-2014 — Закон Королевства Бахрейн № 60 от 30.09.2014 «О преступлениях в области информационных технологий».

Закон ИРИ 2009 г. — Законом ИРИ от 25.05.2009 «О компьютерных преступлениях».

Закон Катара № 14-2014 — Закон Государства Катар № 14 от 02.10.2014 «О борьбе с электронными преступлениями».

Закон Кувейта № 63-2015 — Закон Государства Кувейт № 63 от 07.07.2015 «О борьбе с преступлениями в сфере информационных технологий».

Закон РИ № 1-2023 — Закон Республики Индонезия № 1 от 02.01.2023 «Уголовный кодекс».

Закон РИ № 11-2024 — Закон Республики Индонезия № 11 от 02.01.2024 «О внесении изменений в Закон № 11 2008 г. об электронной информации и транзакциях».

Закон РИ № 21-2000 — Закон Республики Индия № 21 от 09.06.2000 «Об информационных технологиях».

Закон РИ № 44-2023 — Закон Республики Индия № 44 от 24.12.2023 «О телекоммуникациях».

ИИ / AI — искусственный интеллект.

Информационно-технологические правила Республики Индия (Промежуточное руководство и Кодекс цифровых медиа) от 25.02.2021 (в ред. от 06.04.2023) — Информационно-технические правила РИ.

ИКС — информационно-коммуникационная система.

ИРИ — Исламская Республика Иран.

ИС — информационные системы.

ИТ — информационные технологии.

ИТС — информационно-телекоммуникационные сети.

ИХК — Иорданское Хашимитское Королевство.

КБ — Королевство Бахрейн.

КИИ — критическая информационная инфраструктура.

КМ — Королевство Марокко.

КНР — Китайская Народная Республика.

Конвенция АС — Конвенция Африканского союза о кибербезопасности и защите персональных данных (Аддис-Абеба, 27.06.2014).

КСА — Королевство Саудовская Аравия.

КЦД — конфиденциальность, целостность, доступность.

ЛА — Латинская Америка.

ЛАГ — Лига арабских государств.

МВД — министерство внутренних дел.

МИД — министерство иностранных дел.

Министерское решение № 5-2021 РИ — решение Министра коммуникаций и информатики Республики Индонезия № 5 от 01.04.2021 «О внедрении телекоммуникаций».

Мнения КНР 2022 г. — Мнения Верховного народного суда КНР, Высшей народной прокуратуры КНР, Министерства общественной безопасности КНР от 26.08.2022 «По некоторым вопросам применения уголовных процедур при разрешении дел о преступлениях в информационных сетях».

МССУС — международное сотрудничество в сфере уголовного судопроизводства.

МСЭ — Международный союз электросвязи.

НИОКР — научно-исследовательские и опытно-конструкторские работы.

НПА — нормативный правовой (-ые) акт(-ы).

ОАЭ — Объединённые Арабские Эмираты.

ОД/ФТ — отмывание денег и финансирование терроризма.

ОИС — Организация исламского сотрудничества.

ООН — Организация Объединённых Наций.

ОЭЗ — особые экономические зоны.

ОЭСР — Организация экономического сотрудничества и развития.

ПГ/ТЗ — промышленные города и технологические зоны.

ПО — программное обеспечение.

ПОД/ФТ — противодействие отмыванию денег и финансированию терроризма.

Постановление Главы судебной власти ИРИ — Постановление Главы судебной власти ИРИ от 03.08.2014 «Правила сбора и цитирования электронных доказательств».

Положение КСА 2007 г. — Положение Королевства Саудовская Аравия от 27.03.2007 «О борьбе с преступлениями в сфере информатики».

Положение КСА 2013 г. — Положение Королевства Саудовская Аравия от 12.06.2013 «Об уголовных мерах» (в ред. указа короля КСА от 30.12.2021).

Прокламация ФДРЭ № 958/2016 — Прокламация Федеративной Демократической Республики Эфиопия № 958/2016 от 07.07.2016 «О компьютерных преступлениях».

Прокламация ФДРЭ № 1185/2020 — Прокламация Федеративной Демократической Республики Эфиопия № 1185 от 23.03.2020 «О предупреждении и пресечении разжигании ненависти и дезинформации».

ПФР — подразделение финансовой разведки.

РФ — Российская Федерация.

САКХА / СЭСУ — система электронных судебных услуг.

САМП / СУСД — система управления судебными делами.

САР — специальные административные районы.

СЕ — Совет Европы.

СМИ — средства массовой информации.

СО — Султанат Оман.

Соглашение ШОС — Соглашение о сотрудничестве между правительствами государств-членов Шанхайской организации сотрудничества в борьбе с преступностью (Ташкент, 11.06.2010).

ССАГПЗ — Совет сотрудничества арабских государств Персидского залива.

СФЗ — свободные финансовые зоны.

СЭЗ — свободные экономические зоны.

СЭГ/З — специальные экономические города и зоны.

т.н. — так называемый.

ТР — Тунисская Республика.

ТЭК — топливно-энергетический комплекс.

Уведомление ВНР КНР 2021 г. — уведомление Высшей народной прокуратуры КНР от 22.01.2021 «Об издании положений касательно сетевых преступлений, расследуемых народной прокуратурой».

Универсальная конвенция — Конвенция ООН против киберпреступности; Укрепление международного сотрудничества в борьбе с определёнными преступлениями, совершаемыми с использованием информационно-коммуникационных систем, и в обмене доказательствами в электронной форме, относящимися к серьёзным преступлениям.

Указ Министра юстиции, исламских дел и вакфа Королевства Бахрейн № 42-2022 — указ Министра юстиции, исламских дел и вакфа Королевства Бахрейн № 42 от 17.03.2022 «О передаче персональных данных за пределы Королевства Бахрейн».

Указ Султана Омана № 12-2011 — Указа Султана Омана № 12 от 06.02.2011 «О борьбе с преступлениями в сфере информационных технологий».

УНП ООН — Управление по наркотикам и преступности ООН.

УНФПП — Установленные нефинансовые предприятия и лица определенных профессий.

ФАТА — иранская полиция в сфере производства и обмена информацией.

ФДРЭ — Федеративная Демократическая Республика Эфиопия.

ФДЗ — Федеральный декрет-закон.

ФДЗ ОАЭ № 38-2022 — Федеральный декрет-закон ОАЭ № 38 от 30.10.2022 «Об уголовных мерах».

ФДЗ ОАЭ № 34-2021 — Федеральный декрет-закон ОАЭ № 34 от 20.09.2021 «О борьбе со слухами и электронными преступлениями».

ФЗ — Федеральный закон.

ФЛ — физическое лицо.

ФРБ — Федеративная Республика Бразилия.

ШОС — Шанхайская организация сотрудничества.

ЭВМ — электронно-вычислительная машина.

ЭДО — электронный документооборот.

ЭСП — электронное средство платежа.

ЮЛ — юридическое лицо.

ADGMIN — Встреча цифровых министров АСЕАН.

ADGSOM — Встреча цифровых руководящих должностных лиц АСЕАН.

ADM2025 — Генеральный план АСЕАН в сфере ИКТ 2025 года.

ADMM — Встреча министров телекоммуникаций и информационных технологий стран АСЕАН и связанные с ней совещания.

AIM2015 — Генеральный план АСЕАН в сфере ИКТ 2015 года.

AIM2020 — Генеральный план АСЕАН в сфере ИКТ 2020 года.

ATRC — Совет регуляторов телекоммуникаций.

IGAD — Межправительственный орган по развитию.

CIRT — команда реагирования на компьютерные инциденты.

CERT — компьютерная группа реагирования на чрезвычайные ситуации.

CSIRT — команда компьютерной безопасности по реагированию на инциденты.

I4C — Индийский национальный центр кибербезопасности.

PIDA — Политика и регулирующая инициатива для цифровой Африки.

SAFCSP — Саудовская Федерация кибербезопасности, программирования и дронов.

SARA (Tribe, Religion, Race, and Intergroup) — племя, религия, раса, межгруппа.

SCA — Управление по ценным бумагам и сырьевым товарам ОАЭ.

SOMTC — Совещание высших должностных лиц по транснациональной преступности.

TELMIN — Встреча министров обороны стран АСЕАН о развитии оборонного сотрудничества в интересах динамичного сообщества АСЕАН.

TELSOM — Встреча высших должностных лиц по телекоммуникациям и информационным технологиям.

VARA — Управление по регулированию виртуальных активов, регулирующее виртуальные активы в свободных зонах Дубая.

VASP — лица, предлагающие услуги в сфере виртуальных активов.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ И ЛИТЕРАТУРЫ

Международные договоры и соглашения

1. Генеральная Ассамблея ООН: Резолюция 79/243, принятая Генеральной Ассамблеей 24декабря 2024 года «Конвенция Организации Объединенных Наций против киберпреступности; укрепление международного сотрудничества в борьбе с определенными преступлениями, совершаемыми с использованием информационно-коммуникационных систем, и в обмене доказательствами в электронной форме, относящимися к серьезным преступлениям» // Документ ООН A/RES/79/243, 31 December 2024.

2. Соглашение о сотрудничестве между правительствами государств-членов Шанхайской организации сотрудничества в борьбе с преступностью (Ташкент, 11.06.2010) // Шанхайская организация сотрудничества: официальный сайт. — URL: https://rus.sectsco.org/images/07e8/0c/05/1609696.pdf (дата обращения: 09.03.2025).

3. Соглашения между Правительствами государств-членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности (Екатеринбург, 16 июня 2009 г.) // Шанхайская организация сотрудничества: официальный сайт. — URL: https://rus.sectsco.org/20090616/1609633.html (дата обращения: 09.03.2025).

4. African Union Convention on cyber security and personal data protection // African Union: official website. — URL: https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf (accessed 09.03.2025).

5. Convention on Cybercrime (Budapest, 23.XI.2001) // Council of Europe: official website. — URL: https://rm.coe.int/1680081561 (accessed 09.03.2025).

6. الاتفاقية العربية لمكافحة جرائم تقنية المعلومات [Арабская Конвенция о борьбе с преступлениями в области информационных технологий] // Лига арабских государств: официальный сайт. — URL: http://www.lasportal.org/ar/legalnetwork/Documents/التصديق%20على%20الاتفاقية%20العرب%20لمكافحة%20جرائم%20تقنية%20المعلومات.pdf (дата обращения: 09.03.2025).

7. وثيقة الرياض للنظام (القانون) الموحد لمكافحة جرائم تقنية المعلومات لدول مجلس التعاون لدول الخليج العربية [Эр-Риядский документ «Единообразное положение (модельный закон) о борьбе с преступлениями в области информационных технологий для стран Совета сотрудничества арабских государств Персидского залива»] // Электронная библиотека Совета сотрудничества арабских государств Персидского залива: официальный сайт. — URL: https://www.gcc-sg.org/ar-sa/CognitiveSources/DigitalLibrary/Lists/DigitalLibrary/1373542617/القانون%20والقضاء.pdf (дата обращения: 09.03.2025).

8. اتفاقية اليمن وإثيوبيا- اتفاق امني [Соглашение между Йеменом и Эфиопией — Договор о безопасности] // Генеральная прокуратура Республики Йемен:

официальный сайт. — URL: http://agoyemen.net/lib_details.php?id=207 (дата обращения: 20.04.2025).

9. النظام الأساسي لمركز منظمة التعاون الإسلامي للتنسيق والتعاون الشرطي [Основное положение Центра Организации исламского сотрудничества по координации и сотрудничеству полиции] // Организация исламского сотрудничества: официальный сайт. — URL: https://www.oic-oci.org/upload/pages/conventions/ar/oic_policy_5893427_ar.pdf (дата обращения: 09.03.2025).

10. قانون الإمارات العربي الاسترشادي لمكافحة جرائم تقنية المعلومات [Модельный эмиратский арабский закон о борьбе с преступлениями в сфере информационных технологий] // Арабская юридическая сеть ЛАГ: официальный сайт. — URL: http://www.leagueofarabstates.net/ar/legalnetwork/PublishingImages/Lists/TypicalArabLaws/AllItems/11.%20%D9%82%D8%A7%D9%86%D9%88%D9%86%20%D8%A7%D9%84%D8%A5%D9%85%D8%A7%D8%B1%D8%A7%D8%AA%20%D8%A7%D9%84%D8%B9%D8%B1%D8%A8%D9%8A%20%D8%A7%D9%84%D8%A7%D8%B3%D8%AA%D8%B1%D8%B4%D8%A7%D8%AF%D9%8A%20%D9%84%D9%85%D9%83%D8%A7%D9%81%D8%AD%D8%A9%20%D8%AC%D8%B1%D8%A7%D8%A6%D9%85%20%D8%AA%D9%82%D9%86%D9%8A%D8%A9%20%D8%A7%D9%84%D9%85%D8%B9%D9%84%D9%88%D9%85%D8%A7%D8%AA.pdf (дата обращения: 07.04.2025) (на араб. яз.).

11. المذكرة التوضيحية للقانون الجزائي العربي الموحد الجزء الأول [Пояснительная записка к Модельному закону о преступлениях Лиги арабских государств: часть первая] // Электронная база единообразных арабских законов в рамках Лиги арабских государств: официальный сайт. — URL: http://www.lasportal.org/ar/legalnetwork/PublishingImages/Lists/TypicalArabLaws/AllItems/08.%20الموحد%20العربي%20الجزائي%20القانون.pdf (дата обращения: 05.02.2023).

12. Acuerdo entre el Gobierno del Reino de España y el Gobierno del Reino de Marruecos en materia de cooperación policial transfronteriza, hecho "ad referendum" en Madrid el 16 de noviembre de 2010 // Boletín official del estado. 2012. № 116. Sec. I. P. 35412–35416.

13. Convenio entre el Reino de España y el Reino de Marruecos sobre cooperación en materia de seguridad y de lucha contra la delincuencia, hecho en Rabat el 13 de febrero de 2019 // Boletín official del estado. 2022. № 83. Sec. I. P. 46756–46760.

Документы международных органов и организаций

14. Декларация Рио-де-Жанейро «Укрепление сотрудничества Глобального Юга для более инклюзивного и устойчивого управления» (Рио-де-Жанейро, Бразилия, 06.06.2025) // Кремль: официальный сайт. — URL: http://static.kremlin.ru/media/events/files/ru/gvTArkWauqwuryk9xzLt3HuuI7EBmqrC.pdf (дата обращения: 06.07.2025).

15. Руководство по применению риск-ориентированного подхода. Виртуальные активы и провайдеры услуг виртуальных активов // ФАТФ: официальный сайт. — URL: https://www.fatf-gafi.org/content/dam/fatf-

gafi/translations/guidance/MUMCFM-FATF-Guidance-RBA-VA-VASPs.pdf (дата обращения: 08.04.2025).

16. A/AC.291/CRP.8/Rev.1 // UNODC: official website. — URL: https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Second_session/CRP8_Rev1.pdf (accessed 21.04.2025).

17. African Union Child Online Safety and Empowerment Policy // African Union. — URL: https://au.int/sites/default/files/documents/43798-doc-African_Union_Child_Online_Safety_and_Empowerment_Policy_Feb_2024.pdf (accessed 04.05.2025).

18. AFRIPOL cybercrime strategy // Council of Europe: official website. — URL: https://rm.coe.int/afripol-strategy-on-cybercrime-v01-en/1680a30050 (accessed 04.05.2025).

19. AIM2015 // ASEAN: official website. — URL: https://asean.org/wp-content/uploads/images/2012/Economic/TELMIN/ASEAN%20ICT%20Masterplan%202015.pdf (accessed 27.04.2025).

20. AIM2020 // ASEAN. — URL: https://asean.org/wp-content/uploads/images/2015/November/ICT/15b%20--%20AIM%202020_Publication_Final.pdf (accessed 27.04.2025).

21. AIM2025 // ASEAN: official website. — URL: https://asean.org/book/asean-digital-masterplan-2025/ (accessed 27.04.2025).

22. Arab Cybersecurity Strategy 2023–2027 // Ministry of technologies and communications of Tunis: official website. — URL: https://www.mtc.gov.tn/fileadmin/user_upload/Arab_Cybersecurity_Strategy_2023-2027_White_Paper.pdf (accessed 05.05.2025).

23. ASEAN Data Management Framework // ASEAN: official website. — URL: https://asean.org/wp-content/uploads/2021/08/ASEAN-Data-Management-Framework.pdf (accessed 03.05.2025).

24. ASEAN Declaration to prevent and combat cybercrime. Manila, the Philippines, 13 November 2017 // ASEAN: official website. — URL: https://asean.org/wp-content/uploads/2017/11/ASEAN-Declaration-to-Combat-Cybercrime.pdf (accessed 27.04.2025).

25. ASEAN Regional forum statement by the ministers of foreign affairs on cooperation in ensuring cyber security // ASEAN Regional forum: official website. — URL: https://aseanregionalforum.asean.org/wp-content/uploads/2019/01/ARF-Statement-on-Cooperation-in-Ensuring-Cyber-Security.pdf (accessed 27.04.2025).

26. ASEAN REGIONAL FORUM WORK PLAN ON SECURITY OF AND IN THE USE OF INFORMATION AND COMMUNICATIONS TECHNOLOGIES (ICTs) // ASEAN Regional forum: official website. — URL: https://aseanregionalforum.asean.org/wp-content/uploads/2018/07/ARF-Work-Plan-on-Security-of-and-in-the-Use-of-Information-and-Communications-Technologies.pdf (accessed 27.04.2025).

27. ASEAN TELECOMMUNICATIONS AND INFORMATION TECHNOLOGY MINISTERS MEETING (TELMIN) FRAMEWORK ON DIGITAL DATA GOVERNANCE // ASEAN: official website. — URL: https://asean.org/wp-content/uploads/2012/05/6B-ASEAN-Framework-on-Digital-Data-Governance_Endorsedv1.pdf (accessed 03.05.2025).

28. Commonwealth Cyber Declaration, 2018 // Commonwealth: official website. — URL: https://thecommonwealth.org/commonwealth-cyber-declaration-2018 (accessed 07.07.2025).

29. Continental AI Strategy // AU: official website. — URL: https://au.int/sites/default/files/documents/44004-doc-EN-_Continental_AI_Strategy_July_2024.pdf (accessed 04.05.2025).

30. Declaration of the Second Russia–Africa Summit // Summit Africa: official website. — URL: https://summitafrica.ru/en/about-summit/declaration-2023/ (accessed 26.04.2025).

31. Declaration of the First Russia–Africa Summit // Summit Africa: official website. — URL: https://summitafrica.ru/en/about-summit/declaration/ (accessed 26.04.2025).

32. Declaration of the Second Russia–Africa Summit on Cooperation in the Field of International Information Security - Russia-Africa Summit // Ministry of Foreign Affairs of the Russian Federation: official website. — URL: https://oldrussianembassyza.mid.ru/russia-africa-summit/-/asset_publisher/SWhrwjfrWDXU/content/declaration-of-the-second-russia-africa-summit-on-cooperation-in-the-field-of-international-information-security?TSPD_101_R0=08765fb817ab20004bbd9a141c8b68ad300f15a9104506ad179abed1ff184d18e2edab1fac2ba1e7084e61ec07143000716877089 6f014c47d66242242761410f33c7a65277afbcfaef22b918b45646cbdeb612134e9e69902f04a44594f375b (accessed 26.04.2025).

33. Joint Communiqué 47th ASEAN Foreign Ministers' Meeting 8 August 2014 Nay Pyi Taw, Myanmar // ASEAN: official website. — URL: https://asean.org/wp-content/uploads/2012/05/Joint-Communique-of-47th-AMM.pdf (accessed 27.04.2025).

34. Joint Statement of the First Ministerial Conference of the Russia-Africa Partnership Forum (Russian Federation, Sirius Federal Territory, 10 November 2024) // Ministry of Foreign Affairs of the Russian Federation: official website. — 11.11.2024. — URL: https://mid.ru/en/foreign_policy/russia_africa/1980876/?TSPD_101_R0=08765fb817ab2000e9e9350fe5b8ccad71e28b5b34d25b5ceb354a2614c292c2c81296e5b08e326e08b689aaa314300074c1e3f0fd4936a874f19ee6d306dd95051157b166e461d6e2a00f731a052eae620f184963a6cb310125e45db20133e7 (accessed 26.04.2025).

35. Inflection Point: Global Implications of Scam Centres, Underground Banking and Illicit Online Marketplaces in Southeast Asia. UNODC, 2025. 85 p.

36. Quantum Europe Strategy // European Union: official website. — URL: https://digital-strategy.ec.europa.eu/en/library/quantum-europe-strategy (accessed 07.07.2025).

37. Leaders' Declaration on Global Governance of Artificial Intelligence // BRICS: official website. — URL: https://brics.br/en/documents/presidency-documents/250706_brics_ggai_declarationfinal.pdf (accessed 07.07.2025).

38. Status List // African Union: official website. — URL: https://au.int/sites/default/files/treaties/29560-sl-AFRICAN_UNION_CONVENTION_ON_CYBER_SECURITY_AND_PERSONAL_DATA_PROTECTION.pdf (accessed 09.03.2025).

39. THE DIGITAL TRANSFORMATION STRATEGY FOR AFRICA (2020-2030) // AU: official website. — URL: https://au.int/sites/default/files/documents/38507-doc-dts-english.pdf (accessed 04.05.2025).

40. Work Programme to Implement the ASEAN Plan of Action to Combat Transnational Crime Kuala Lumpur, 17 May 2002 // ASEAN: official website. — URL: https://asean.org/work-programme-to-implement-the-asean-plan-of-action-to-combat-transnational-crime-kuala-lumpur-17-may-2002/ (accessed 26.04.2025).

41. 1st ASEAN DIGITAL MINISTERS' MEETING (ADGMIN) 2020 IMPLEMENTING GUIDELINES FOR ASEAN DATA MANAGEMENT FRAMEWORK AND ASEAN CROSS BORDER DATA FLOWS MECHANISM // ASEAN: official website. — URL: https://asean.org/wp-content/uploads/2021/08/Implementing-Guidelines-for-ASEAN-Data-Management-Framework-and-Cross-Border-Data-Flows.pdf (accessed 03.05.2025).

42. 2006 ASEAN Regional forum statement on cooperation in fighting cyber attack and terrorist misuse of cyber space // CIL. — URL: https://cil.nus.edu.sg/databasecil/2006-asean-regional-forum-statement-on-cooperation-in-fighting-cyber-attack-and-terrorist-misuse-of-cyber-space/ (accessed 27.04.2025).

43. التصديق على الاتفاقيه العربية لمكافحة جرائم تقنية المعلومات [Ратификация Арабской конвенции о борьбе с преступлениями в области информационных технологий] // Лига арабских государств: официальный сайт. — URL: http://www.leagueofarabstates.net/ar/legalnetwork/Documents/التصديق%20على%20الاتفاقيه%20العربية%20لمكافحة%20جرائم%20تقنية%20المعلومات.pdf (дата обращения: 09.03.2025).

44. الاستراتيجية العربية الامن السيبراني ٢٠٢٣-٢٠٢٧ [Арабская стратегия по кибербезопасности 2023–2027] // Арабская организация информационно-коммуникационных технологий. URL: https://www.aicto.org/publications/studies/#flipbook-df_6464/1/ (дата обращения: 05.06.2025).

Нормативные правовые акты

45. Закон № 04-09 от 25 шабан 1430 года хиджра, что соответствует 16 августа 2009 г. «Специальные правила по предупреждению и борьбе с преступлениями, связанными с информационно-коммуникационными

технологиями» // Официальный вестник Алжирской Республики. — 2009. — № 47. — С. 5–8 (на араб. яз.).

46. Закон АНДР № 04-18 от 25.12.2004 «О профилактике и предотвращении незаконного употребления и незаконного оборота наркотических средств и психотропных веществ» [قانون رقم ٠٤-١٨ مؤرخ في ١٣ ذي القعدة ١٤٢٥ الموافق ٢٥ ديسمبر سنة ٢٠٠٤، يتعلق بالوقاية من المخدرات والمؤثرات العقلية وقمع الاستعمال والاتجار غير المشروعين بها] // Официальный вестник Алжирской Республики. — 2004. — № 83. — С. 3–8.

47. Закон АНДР № 05-23 от 07.05.2023 [القانون رقم ٢٣-٠٥ المؤرخ في ٧ مايو سنة ٢٠٢٣] // Официальный вестник Алжирской Республики. — 2023. — № 32. — С. 13–17.

48. Законопроект № 902782-8. О внесении изменений в статью 104-1 Уголовного кодекса Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации (об особенностях изъятия цифровой валюты) // Система обеспечения законодательной деятельности: официальный сайт. — URL: https://sozd.duma.gov.ru/bill/902782-8 (дата обращения: 20.06.2025).

49. Прокламация ФДРЭ № 958/2016 «О компьютерных преступлениях» // Федеральная газета Негарит. — 2016. — № 83. — С. 9104–9131 (на англ. яз.).

50. Распоряжение Правительства РФ от 11 июля 2023 г. N 1856-р «Об утверждении Концепции регулирования отрасли квантовых коммуникаций в РФ до 2030 г.» // Собрание законодательства Российской Федерации. — 2023. — № 30. — Ст. 5712.

51. Федеральный закон от 6 марта 2006 г. № 35-ФЗ «О противодействии терроризму» // Собрание законодательства Российской Федерации. — 2006. — № 11. — Ст. 1146.

52. Федеральный закон от 25 декабря 2008 г. № 273-ФЗ «О противодействии коррупции» // Собрание законодательства Российской Федерации. — 2008. — № 52 (часть I). — Ст. 6228.

53. Федеральный закон от 25 июля 2002 г. № 114-ФЗ «О противодействии экстремистской деятельности» // Собрание законодательства Российской Федерации. — 2002. — № 30. — Ст. 3031.

54. Anti-Terrorism Proclamation No. 652/2009 // Federal Negarit Gazeta. — 2009. — № 47. — P. 4827–4842.

55. Bharatiya Nyaya Sanhita 2023 // Ministry of Home Affairs: official website. — URL: https://www.mha.gov.in/sites/default/files/250883_english_01042024.pdf (accessed 25.03.2025).

56. Criminal Code of the Federal Democratic Republic of Ethiopia // Federal Negarit Gazeta. — Proclamation No. 414/2004.

57. Crypto-Asset Module. Rulebook of the Central Bank of Bahrain // Central Bank of Bahrain: official website. — URL:

https://cbben.thomsonreuters.com/sites/default/files/net_file_store/Vol_6_CRA_2023.pdf (accessed 08.04.2025).

58. Global AI Hub Law // Istitlaa platform: website. — URL: https://istitlaa.ncc.gov.sa/en/transportation/citc/globalailaw/Documents/Global%20AI%20Hub%20Law%20EN-AR%20-%20Final%20Draft%20for%20PC.pdf (accessed 18.05.2025).

Indian Evidence Act, 1872 // Digital Repository of Laws: website. — URL: https://www.indiacode.nic.in/bitstream/123456789/15351/1/iea_1872.pdf (accessed 19.03.2025).

59. Information Network Security Agency Reestablishment Proclamation No. 808/2013 // Federal Negarit Gazette. — 2014. — No. 6. — P. 7129–7136.

60. Law No. (4) of 2022 Regulating Virtual Assets in the Emirate of Dubai // VARA: website. — URL: https://rulebooks.vara.ae/sites/default/files/en_net_file_store/VARA_EN_338_VER1.pdf (accessed 25.03.2025).

61. Law No. 2 of 2023 on the establishment of RAK Digital Assets Oasis // RAK Legislative Committee: website. — URL: https://www.rak.ae/wps/portal/rak/legislative-committee/legislation-search/!ut/p/z1/jZBBD4IwDIV_Eek2yNyO00TQZKJZRLeLWXTikgkkIr9fIF5Be2v7vb6XgoEzmMp2vrStrysb-l4bemFZSkmKiMzXcYwOuOAipzxVlMJpBBKMCeEJlgwxjsRW4aJYLXHGEjD_6NFECfRbb2aRDf0CcxFHYCaDchXoPuhi0kYmoIY7wZX-Fcbv7WrQBJE4IhEZVvY6TEHf3N2-Q9vY0kHzPJ6R3z-aTooP_T4FDQ!!/ (accessed 25.03.2025).

62. Notification. New Delhi, 27.10.2009 // India Code: Digital Repository of Laws: website. — URL: https://upload.indiacode.nic.in/showfile?actid=AC_CEN_45_76_00001_200021_1517807324077&type=rule&filename=blocking_for_access_of_information_rule_2009.pdf (accessed 02.05.2025).

63. Notification. New Dehli, 11.04.2011 // India Code: Digital Repository of Laws: website. — URL: https://upload.indiacode.nic.in/showfile?actid=AC_CEN_45_76_00001_200021_1517807324077&type=rule&filename=Information%20TechnologyGuidelines%20for%20Cyber%20Cafe%20Rules)%20Rules,%202011%20.pdf (accessed 02.05.2025).

64. Order (42) of 2022 of Ministry of Justice, Islamic Affairs and Waqf. Regarding the transfer of personal data outside the Kingdom of Bahrain // Ministry of Justice, Islamic Affairs and Waqf: website. — URL: http://www.pdp.gov.bh/en/assets/pdf/executive-decisions/eng/trans-order-countries-and-territories-with-adequate-protection-en.pdf (accessed 25.03.2025).

65. PROCLAMATION No. 1148/2019 PROCLAMATION FOR COMMUNICATION SERVICES // Ethiopian Communications Authority: website. —

URL: https://eca.et/wp-content/uploads/2024/05/Communications-Service-Proclamation-No.-1148-2019.pdf (accessed 02.05.2025).

66. PROCLAMATION No. 1321/2024 PROCLAMATION TO PROVIDE FOR PERSONAL DATA PROTECTION // Ethiopian Communications Authority: website. — URL: https://eca.et/wp-content/uploads/2024/10/personal_data_protection_proclamation_No_1321_2024.pdf (accessed 02.05.2025).

67. Proclamation No. 1284/2023 Ethiopian Digital Identification Proclamation // Federal Negarat Gazette. — 2023. — № 19. — P. 14715.

68. Proclamation No. 1185/2020 Hate Speech and Disinformation Prevention and Suppression Proclamation // Federal Negarat Gazette. — 2020. — № 26. — P. 12339.

69. Proclamation No.759/2012 Advertisement Proclamation // Federal Negarat Gazette. — 2012. — № 59. — P. 6520.

70. The Digital Personal Data Protection Act No. 22 of 2023 // The Gazette of India Extraordinary. — 2023. — № 25. — P. 1–21.

71. The Indian Penal Code // Digital Repository of Laws: website. — URL: https://www.indiacode.nic.in/repealedfileopen?rfilename=A1860-45.pdf (accessed 25.03.2025).

72. The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 // India Code: Digital Repository of Laws: website. — URL: https://upload.indiacode.nic.in/showfile?actid=AC_CEN_45_76_00001_200021_1517807324077&type=rule&filename=information_technology_(intermediary_guidelines_and_digital_media_ethics_code)_rules,_2021_(updated_06.04.2023)-.pdf (accessed 02.05.2025).

73. The Prevention of Money-Laundering Act, 2002 // India Code: Digital Repository of Laws: website. — URL: https://www.indiacode.nic.in/bitstream/123456789/2036/5/A2003-15.pdf (accessed 21.04.2025).

74. Telecommunications Act 2023 // India Code: Digital Repository of Laws: website. — URL: https://www.indiacode.nic.in/bitstream/123456789/20101/1/A2023-44.pdf (accessed 10.05.2025).

75. Virtual Assets and Related Activities Regulations 2023 // VARA: website. — URL: https://rulebooks.vara.ae/node/18 (accessed 25.03.2025).

76. Pencegahan dan Pemberantasan Tindak Pidana Pendanaan Terorisme [О предупреждении и искоренении уголовного преступления финансирования терроризма] // Законодательная база Республики Индонезия: официальный сайт. — URL: https://peraturan.bpk.go.id/Details/38846/uu-no-9-tahun-2013 (дата обращения: 09.02.2025).

77. Penanganan Bantuan Timbal Balik dalam Masalah Pidana di Lingkungan Kementerian Hukum dan Hak Asasi Manusia [Обработка взаимной помощи по

уголовным вопросам в Министерстве права и прав человека] // Законодательная база Республики Индонезия: официальный сайт. — URL: https://peraturan.bpk.go.id/Details/225563/permenkumham-no-12-tahun-2022 (дата обращения: 09.02.2025).

78. Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik [Закон Республики Индонезия № 11 2008 г. «Об электронной информации и трансакциях»] // База законодательства Республики Индонезия: официальный сайт. — URL: https://peraturan.bpk.go.id/Details/37582/uu-no-19-tahun-2016 (дата обращения: 19.03.2025).

79. Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik [О внесении изменений в Закон № 11 2008 г. об информации и электронных сделках] // Законодательная база Республики Индонезия: официальный сайт. — URL: https://peraturan.bpk.go.id/details/274494/uu-no-1-tahun-2024 (дата обращения: 04.05.2025).

80. Peraturan Menteri Komunikasi dan Informatika Nomor 5 Tahun 2021 tentang Penyelenggaraan Telekomunikasi [Решение министра коммуникаций и информатики номер 5 от 2021 года о внедрении телекоммуникаций] // Министерство коммуникаций и информатики Республики Индонезия: официальный сайт. — URL: https://jdih.komdigi.go.id/produk_hukum/view/id/768/t/peraturan+menteri+komunikasi+dan+informatika+nomor+5+tahun+2021 (дата обращения: 04.05.2025).

81. Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik [Правительственное постановление номер 71 2019 года о внедрении электронных систем и транзакций] // Министерство телекоммуникаций и информатики Республики Индонезия: официальный сайт. — URL: https://jdih.komdigi.go.id/produk_hukum/view/id/695/t/peraturan+pemerintah+nomor+71+tahun+2019+tanggal+10+oktober+2019 (дата обращения: 04.05.2025).

82. Regulation of the President of the Republic of Indonesia Number 47 Of 2023 On National Cyber Security Strategy And Cyber Crisis Management // Peraturan: website. — URL: https://peraturan.go.id/files2/perpres-no-47-tahun-2023_terjemah.pdf (accessed 05.04.2025).

83. Undang-undang (UU) Nomor 1 Tahun 1979 tentang Ekstradisi [Закон Республики Индонезия от 18.01.1979 «О выдаче»] // Законодательная база Республики Индонезия: официальный сайт. — URL: https://peraturan.bpk.go.id/Details/47145/uu-no-1-tahun-1979 (дата обращения: 09.02.2025).

84. Undang-undang (UU) Nomor 27 Tahun 2022 Pelindungan Data Pribadi [Закон № 27 «О защите персональных данных» 2022 г.] // Официальная база законодательства РИ: сайт. — URL: https://peraturan.bpk.go.id/Details/229798/uu-no-27-tahun-2022 (дата обращения: 27.04.2025).

85. Undang-undang (UU) Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana [Закон Республики Индонезия № 1 от 02.01.2023 «Уголовный кодекс»] // Законодательная база Республики Индонезия: сайт. — URL: https://peraturan.bpk.go.id/Details/234935/uu-no-1-tahun-2023 (дата обращения: 10.02.2025).

86. Undang-undang (UU) Nomor 8 Tahun 1981 tentang Hukum Acara Pidana [Закон Республики Индонезия № 8 от 31.12.1981 «Уголовно-процессуальный кодекс»] // Законодательная база Республики Индонезия: сайт. — URL: https://peraturan.bpk.go.id/Details/47041/uu-no-8-tahun-1981 (дата обращения: 10.02.2025).

87. Undang-undang (UU) Nomor 1 Tahun 2006 tentang Bantuan Timbal Balik dalam Masalah Pidana [Закон Республики Индонезия № 1 от 03.03.2006 «О взаимной правовой помощи по уголовным делам»] // Законодательная база Республики Индонезия: сайт. — URL: https://peraturan.bpk.go.id/Details/40151/uu-no-1-tahun-2006 (дата обращения: 09.02.2025).

88. القانون رقم ٨٨.١٣ المتعلق بالصحافة والنشر الصادر بظهير شريف رقم ١.١٦.١٢٢ صادر في ٦ ذي القعدة ١٩٣٧ (١٠) أغسطس ٢٠١٦ // الجريدة الرسمية. ٢٠١٦. ١١. ٥٩٦٦-٥٩٨٧ ص. [Закон № 88.13 «О прессе и издательском деле», изданный Королевским указом № 1.16.122 от 6 зуль-кида 1937 (10) августа 2016 г. // Официальный вестник. — 2016. — № 11. — С. 5966-5987.]

89. قانون رقم ٣٠ لسنة ٢٠١٨ بإصدار قانون حماية البيانات الشخصية [Закон Королевства Бахрейн № 30 от 12.07.2018 «О персональных данных»] // Комиссия по законодательству и юридическим заключениям Королевства Бахрейн: сайт. — URL: https://www.legalaffairs.gov.bh/HTM/K3018.htm (дата обращения: 25.03.2025).

90. قانون اتحادي رقم (2) لسنة 2019 في شأن استخدام تقنية المعلومات والاتصالات في المجالات الصحية [Федеральный закон Объединённых Арабских Эмиратов № 2 от 2019 года «Об использовании информационно-телекоммуникационных технологий в сфере здравоохранения»] // Официальная база законодательства ОАЭ: сайт. — URL: https://uaelegislation.gov.ae/ar/legislations/1209 (дата обращения: 01.04.2025).

91. آیین نامه جمع آوری و استنادپذیری ادله الکترونیکی [Правила сбора и цитирования электронных доказательств] // Законодательная база ИРИ: сайт. — URL: https://rc.majlis.ir/fa/law/show/897504 (дата обращения: 04.04.2025).

92. نظام الإعلام المرئي والمسموع [Положение «Об аудио-визуальных СМИ»] // Бюро экспертов Совета министров КСА: сайт. — URL: https://laws.boe.gov.sa/BoeLaws/Laws/LawDetails/ed5fdbc0-c183-4a8a-a8b7-a9ed004b5900/1 (дата обращения 02.05.2025).

93. نظام المطبوعات والنشر [Положение «О печати и публикациях»] // Библиотека Министерства СМИ Королевства Саудовская Аравия: сайт. — URL: https://www.media.gov.sa/sites/default/files/2020-06/نظام%20المطبوعات%20والنشر.pdf (дата обращения: 15.02.2025).

94. قانون اتحادي رقم ٢ لسنة ٢٠٠٦ م في شأن مكافحة جرائم تقنية المعلومات [Федеральный закон Объединённых Арабских Эмиратов № 2 2006 года «О борьбе с преступлений в сфере информационных технологий»] // Официальная онлайн база законодательства ОАЭ: сайт. — URL: https://elaws.moj.gov.ae/UAE-MOJ_OG/10002S_2006/01-31-2006_0442/UAE-OG_2006-01-30_00002_kait.pdf (дата обращения: 18.03.2025).

95. مرسوم بقانون اتحادي رقم ٣٤ لسنة ٢٠٢١ في شأن مكافحة الشائعات والجرائم الإلكترونية [Федеральный декрет-закон Объединённых Арабских Эмиратов № 34 2021 года «О борьбе со слухами и электронными преступлениями] // Официальная онлайн база законодательства ОАЭ: сайт. — URL: https://uaelegislation.gov.ae/ar/legislations/1526 (дата обращения: 10.03.2025).

96. ظهير شريف رقم ١.٢٠.٦٩ صادر في ٤ ذي الحجة ١٤٤١ (٢٥) يوليو بتنفيذ القانون رقم ٠٥.٢٠ المتعلق بالأمن السيبراني [Королевский указ № 1.20.69, изданный 04.12.1441, соответствующий 25.07.2020 «Об издании закона № 05.20 касающегося кибербезопасности»] // Официальный вестник. — 2020. — № 6904. — С. 4160–4167.

97. مقترح قانون عدد ٠٣٦/٢٠٢٤ يتعلق بالأمن السيبراني [Предлагаемый закон № 036/2024 о кибербезопасности] // Собрание народных представителей Тунисской Республики: сайт. — URL: https://www.arp.tn/ar_SY/document/download/100242 (дата обращения: 09.03.2025).

98. قانون رقم ٠٤-٠٩ مؤرخ في ١٤ شعبان عام ١٤٣٠ الموافق ٥ غشت سنة ٢٠٠٩، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها. [Закон № 04-09 от 14.08.1430, соответствующий 05.08.2009, включающий специальные правила по предупреждению и борьбе с преступлениями, связанными с информационно-коммуникационными технологиями] // Официальный вестник Алжирской Республики. — 2009. — № 47. — С. 5–8.

99. قانون رقم ٠٧.٠٣ بتتميم مجموعة القانون الجنائي في ما يتعلق بالجرائم المتعلقة بنظم المعالجة الآلية للمعطيات [Закон № 07.03, дополняющий свод уголовного закона в части преступлений, связанных с автоматизированными системами обработки данных] // Официальный вестник. — 2003. — № 5171. — С. 4284–4285.

100. قانون رقم ١٤ لسنة ٢٠١٤ بإصدار قانون مكافحة الجرائم الإلكترونية [Закон Государства Катар № 14 от 02.10.2014 «О борьбе с электронными преступлениями»] // Законодательства база Государства Катар «Al-Meezan». URL: https://www.almeezan.qa/LawPage.aspx?id=6366&language=ar (дата обращения: 09.03.2025).

101. قرار مجلس الوزراء رقم (42) لسنة 2025 بشأن لائحة المخالفات والجزاءات الإدارية المرتبطة بتنظيم الإعلام [Постановление Совета министров ОАЭ № 42 от 2025 года «О регулировании административных правонарушений и наказаний, связанных с регулированием деятельности средств массовой информации»] // Совет ОАЭ по СМИ: сайт. — URL: https://uaemc.gov.ae/violations-and-penalties/ (дата обращения:21.06.2025).

102. نظام مكافحة جرائم المعلوماتية ١٤٢٨ [Положение Королевства Саудовская Аравия от 27.03.2007 «Борьба с преступлениями в сфере информатики»] // Бюро

экспертов Совета министров Королевства Саудовская Аравия: сайт. — URL: https://laws.boe.gov.sa/BoeLaws/Laws/LawDetails/25df73d6-0f49-4dc5-b010-a9a700f2ec1d/1 (дата обращения: 09.03.2025).

103. قانون رقم ٦٣ لسنة ٢٠١٥ في شأن مكافحة جرائم تقنية المعلومات [Закон Государства Кувейт № 63 2015 года «О борьбе с преступлениями в сфере информационных технологий»] // Электронное правительство Государства Кувейт: сайт. — URL: https://www.e.gov.kw/sites/kgoarabic/Forms/CAITLawNo.63of2015oncombatingInformationTechnologyCrimes.pdf (дата обращения: 09.03.2025).

104. قانون رقم ٦٠ لسنة ٢٠١٤ بشأن جرائم تقنية المعلومات [Закон Королевства Бахрейн № 60 от 30.09.2014 «О преступлениях в области информационных технологий»] // Комитет по законодательству и правовому мнению Королевства Бахрейн: сайт. — URL: https://www.lloc.gov.bh/Legislation/HTM/K6014 (дата обращения: 10.03.2025).

105. مرســـوم سلطاني رقـم ٢٠١١/١٢ بإصدار قانون مكافحة جرائم تقنية المعلومات [Указ Султана Омана № 12 2011 года «О борьбе с преступлениями в сфере информационных технологий»] // Министерство юстиции и правовым вопросам Султаната Оман: сайт. — URL: https://mjla.gov.om/legislation/decrees/details.aspx?Id=213&type=L&lang=a (дата обращения: 09.03.2025).

106. مرسوم بقانون اتحادي بإصدار قانون المعاملات التجارية [Федеральный декрет-закон о коммерческих сделках] // Законодательная база ОАЭ: сайт. — URL: https://uaelegislation.gov.ae/ar/legislations/1610 (дата обращения: 29.09.2024).

107. مرسوم بقانون اتحادي في شأن الشركات التجارية [Федеральный декрет-закон о коммерческих компаниях] // Законодательная база ОАЭ: сайт. — URL: https://uaelegislation.gov.ae/ar/legislations/1542 (дата обращения: 29.09.2024).

108. مرسوم بقانون اتحادي بشأن المشروعات ذات الصفة المستقبلية [Федеральный декрет-закон о будущих проектах] // Законодательная база ОАЭ: сайт. — URL: https://uaelegislation.gov.ae/ar/legislations/1980 (дата обращения: 29.09.2024).

109. مرسوم بقانون اتحادي في شأن التجارة من خلال وسائل التقنية الحديثة [Федеральный декрет-закон о торговле с помощью современных технологий] // Законодательная база ОАЭ: сайт. — URL: https://uaelegislation.gov.ae/ar/legislations/2150 (дата обращения: 29.09.2024).

110. قانون مكافحة جرائم تقنية المعلومات رقم ١٧٥ لسنة ٢٠١٨ [Закон № 175 от 2018 года «О борьбе с преступлениями в сфере информационных технологий»] // Официальный вестник. — 2018. — №32.2 (д). — С. 3–25.

111. قانون رقم ١١ لسنة ٢٠٠٤ بإصدار قانون العقوبات [Закон Государства Катар № 11 от 10.05.2004 «Наказания»] // Законодательства база Государства Катар «Al-Meezan». URL: https://www.almeezan.qa/LawPage.aspx?id=26&language=ar (дата обращения: 09.03.2025).

112. قانون رقم ٦٠ لسنة ٢٠١٤ بشأن جرائم تقنية المعلومات [Закон Королевства Бахрейн № 60 от 30.09.2014 «О преступлениях в области информационных технологий»] // Комиссия по законодательству и юридическому заключению Королевства

Бахрейн: сайт. — URL: https://www.lloc.gov.bh/Legislation/HTM/K6014 (дата обращения: 09.03.2025).

113. مرســـوم سلطاني رقـم ٢٠١١/١٢ بإصدار قانون مكافحة جرائم تقنية المعلومات [Указ Султана Омана № 12 2011 года «О борьбе с преступлениями в сфере информационных технологий»] // Министерство юстиции и правовым вопросам Султаната Оман: сайт. — URL: https://mjla.gov.om/legislation/decrees/details.aspx?Id=213&type=L&lang=a (дата обращения: 09.03.2025).

114. قانون اتحادي رقم ٥١ صادر بتاريخ ٢٠٠٦/١١/٠٩ م في شأن مكافحة جرائم الاتجار بالبشر [Федеральный закон ОАЭ № 51 от 09.11.2006 «О борьбе с преступлениями, связанными с торговлей людьми» (в ред. ФЗ № 1 от 15.01.2015)] // Официальная онлайн база законодательства ОАЭ: сайт. —. URL: https://elaws.moj.gov.ae/UAE-MOJ_OG/10002S_2006/11-14-2006_0457/UAE-OG_2006-11-09_00051_kait.pdf (дата обращения: 18.03.2025).

115. قانون العقوبات رقم ١٦ لسنة ١٩٦٠م مقام [Закон № 16 «О преступлениях» 1960 г.] // Министерство юстиции Иорданского Хашимитского Королевства: сайт. — URL: https://www.moj.gov.jo/ebv4.0/root_storage/ar/eb_list_page/قانون_العقوبات_وتعديلاته_رقم_6_لسنة_1960.pdf (дата обращения: 25.03.2025).

116. مرسوم بقانون اتحادي رقم ٣١ لسنة ٢٠٢١ بإصدار قانون الجرائم والعقوبات [Федеральный декрет-закон Объединённых Арабских Эмиратов № 31 от 20.09.2021 «Преступления и наказания»] // Официальный сайт Комитета министров ОАЭ: сайт. — URL: https://laws.uaecabinet.ae/ar/materials/law/1529?page=1 (дата обращения: 25.03.2025).

117. نظام مكافحة جرائم الإرهاب وتمويله [Положение «О борьбе с террористическими преступлениями и его финансированием»] // Бюро экспертов Совета министров Королевства Саудовская Аравия: сайт. — URL: https://laws.boe.gov.sa/BoeLaws/Laws/LawDetails/57694209-3eed-46c7-a5d8-a9ed012761d4/1 (дата обращения: 25.03.2025).

118. قانون آیین دادرسی کیفری مصوب ۱۲.۰۴.۱۳۹۲[Уголовно-процессуальный закон Ирана, принятый 12.04.1392] // База законодательства ИРИ: сайт. — URL: https://www.davoudabadi.ir/9673250/قانون-آیین-دادرسی-کیفری (дата обращения: 04.04.2025).

119. قانون مجازات اسلامی [Исламский уголовный закон] // Законодательная база: сайт. — URL: https://davoudabadi.ir/page/5709812/قانون-مجازات-اسلامی (дата обращения: 19.04.2025).

120. مرسوم بقانون ١٥ لسنة ١٩٧٦ بإصدار قانون العقوبات [Декрет-закон Королевства Бахрейн № 15 1976 года «О наказаниях»] // Электронная база законодательства Королевства Бахрейн: сайт. — URL: https://www.legalaffairs.gov.bh/Publications/Download/017.pdf (дата обращения: 31.01.2025).

121. قرار المجلس التنفيذي رقم ٣ لسنة ٢٠١٩ بشأن تنظيم التجربة التشغيليّة للمركبة ذاتيّة القيادة في إمارة دبي [Решение Исполнительного совета Эмирата Дубай № 3 от 17.04.2019 «Об организации эксплуатации беспилотных транспортных средств в Эмирате Дубай»] // Законодательный портал Дубай: сайт. — URL: https://dlp.dubai.gov.ae/Legislation%20Ar%20Reference/2019/قرار%20المجلس%20التنفيذي%20رقم%20(3)%20لسنة%202019%20بشأن%20تنظيم%20ذاتية%20القيادة%20مركبة%.html#:~:text=ن&text=20.تعمل%20بمُوجب%20نظام%20المُحاكاة,فيها%20المُواصفات%20التي%20تعتمدها%20الهيئة%20نظام%20إلكتروني%20ذكي%20مُصمّم%20من,قيادتها%20بدون%20أي%20تدخُّل%20بشري (дата обращения: 25.03.2025).

122. قانون رقم ٩ لسنة ٢٠٢٣ بشأن تنظيم تشغيل المركبات ذاتيّة القيادة في إمارة دبي [Закон Эмирата Дубай № 9 от 2023 г. «Об эксплуатации беспилотных транспортных средств в Эмирате Дубай»] // Законодательный портал Дубай: сайт. — URL: https://dlp.dubai.gov.ae/Legislation%20Ar%20Reference/2023/20%(9)20%قانون%20رقم%20لسنة%202023%20بشأن%20تنظيم%20تشغيل%20المركبات%20ذاتية%20القيادة.pdf (дата обращения: 25.03.2025).

123. قانون جرائم رايانه ای [Закон о компьютерных преступлениях // Исследовательский центр Исламского совета ИРИ: сайт. — URL: https://rc.majlis.ir/fa/law/show/135717 (дата обращения: 09.03.2025).

124. مرسوم سلطاني رقم ٥٨ / ٢٠٢٤ بإصدار قانون الإعلام [Указ Султана № 58/2024 об обнародовании Закона о СМИ] // Законодательная база «Кануун»: сайт. — URL: https://qanoon.om/p/2024/rd2024058/ (дата обращения: 04.05.2025).

125. تنظيم الهيئة السعودية للمدن الصناعية ومناطق التقنية [Положение о Саудовском управлении промышленных городов и технологических зон] // Бюро экспертов Совета министров КСА: сайт. — URL: https://laws.boe.gov.sa/BoeLaws/Laws/LawDetails/f9bd197e-980e-4e9f-948c-a9a700f2994e/1 (дата обращения: 25.03.2025).

126. (تنظيم هيئة المدن الاقتصادية (هيئة المدن والمناطق الاقتصادية الخاصة [Положение об Управлении экономических городов (Управлении специальных экономических городов и зон)] // Бюро экспертов Совета министров КСА: сайт. — URL: https://laws.boe.gov.sa/BoeLaws/Laws/LawDetails/4100e06a-1a43-458d-a3b4-a9a700f1e3d9/1 (дата обращения: 25.03.2025).

127. قانون تصنيف وثائق الدولة وتنظيم الأماكن المحمية [указ Султана Оман № 118/2011 «Закон о классификации государственных документов и регулировании охраняемых мест»] // Законодательная база «Кануун»: сайт. — URL: https://qanoon.om/p/2011/l2011118/ (дата обращения: 25.03.2025).

128. مرسوم سلطاني رقم ٦ / ٢٠٢٢ بإصدار قانون حماية البيانات الشخصية [указ Султана Оман № 6/2022 «Закон о защите персональных данных»] // Законодательная база «Кануун»: сайт. — URL: https://qanoon.om/p/2011/l2011118/ (дата обращения: 02.05.2025).

129. وزارة النقل والاتصالات وتقنية المعلومات: قرار وزاري رقم ٣٤ / ٢٠٢٤ بإصدار اللائحة التنفيذية لقانون حماية البيانات الشخصية [Министерство транспорта, коммуникаций и информационных технологий: Министерское решение № 34/2024 об издании

Исполнительного регламента Закона о защите персональных данных] // Законодательная база «Кануун»: сайт. — URL: https://qanoon.om/p/2011/l2011118/ (дата обращения: 02.05.2025).

130. مرسوم بقانون اتحادي في شأن حماية البيانات الشخصية [Федеральный декрет-закон ОАЭ № 712 от 20.09.2021 «О защите персональных данных»] // Официальная база законодательства ОАЭ. URL: https://uaelegislation.gov.ae/ar/legislations/1972?keyword= (дата обращения: 25.03.2025).

131. اللائحة التنفيذية لنظام حماية البيانات الشخصية [Исполнительные правила к Положению о защите персональных данных] // Национальная платформа управления данными КСА: сайт. — URL: https://dgp.sdaia.gov.sa/wps/portal/pdp/knowledgecenter/details/PDPL2/!ut/p/z1/jY-xDoIwFEW_xQ8gfS1Q61gEIgpaUkDsYhgESbQQQxz8ehsGB6Pi215yTu69SKESKV3d26Ya2k5XF_MfFD2S1OfYczAWpAiBcpZmxS4lcuGi_QhEPKArLIEIurWBspTZLJgDgIvUPz58OQ5T_noKMAvILVkmDVJ9NZytVtcdKoUvYmLC1ai_6mOcM1M_2dAszDF4zjvwYd8I_BggTxr117x8xLWMLD57As174Bg!/dz/d5/L0lHSkovd0RNQU5rQUVnQSEhLzROVkUvYXI!/ (дата обращения: 10.05.2025).

132. الدليل الإسترشادي للتعاون القضائي الدولي في المسائل الجنائية [Руководящие принципы международного судебного сотрудничества по уголовным делам] // Министерство юстиции ОАЭ: сайт. — URL: https://www.moj.gov.ae/Content/Userfiles/Assets/Documents/8e8f1221.pdf (дата обращения: 08.04.2025).

133. نظام المحاكم التجارية [Положение «О коммерческих судах»] // Бюро экспертов Совета министров КСА: сайт. — URL: https://laws.boe.gov.sa/BoeLaws/Laws/LawDetails/38334008-3b70-4c6c-b3af-aba3016a8061/1 (дата обращения: 09.03.2025).

134. نظام نقل معلومات المتعاملين مع المنشآت الخاصة إلكترونياً إلى مركز المعلومات الوطني في وزارة الداخلية (نظام شموس الأمني) [Положение КСА от 21.04.2014 «О передаче информации о клиентах с частными средствами в Национальный информационный центр при Министерстве внутренних дел (Система безопасности Шумуусун)»] // Бюро экспертов Совета министров КСА: сайт. — URL: https://laws.boe.gov.sa/BoeLaws/Laws/LawDetails/ad0354f7-9756-4a4e-8948-a9a700f19705/1 (дата обращения: 25.03.2025).

135. ضوابط إجراءات الإثبات إلكترونياً [решение Министра юстиции КСА № 921 от 12.10.2022 «Контроль процедур электронного доказательства»] [Электронный ресурс] // Министерство юстиции КСА: сайт. — URL: https://laws.moj.gov.sa/legislation/ps6CWt8A6oJ1b6j+n6vr%2Fw== (дата обращения: 19.03.2025).

136. الأدلة الإجرائية لنظام الإثبات [Процедурные руководства к Положению о доказательствах КСА от 12.10.2022] // Министерство юстиции КСА: сайт. — URL: https://laws.moj.gov.sa/legislation/8ST%2Fur3URoFaiLSA0IAGGw==#content-card-VeTqvtWGcIOGGQvMXQ (дата обращения: 25.03.2025).

137. نظام الإثبات [Положение Королевства Саудовская Аравия от 07.01.2022 «О доказательствах»]. // Бюро экспертов Совета министров КСА: сайт. — URL: https://laws.boe.gov.sa/BoeLaws/Laws/LawDetails/2716057c-c097-4bad-8e1e-ae1400c678d5/1 (дата обращения: 09.03.2025).

138. قانون اتحادي رقم ١ لسنة ٢٠٠٦م في شأن المعاملات والتجارة الإلكترونية [Федеральный закон ОАЭ № 1 от 2006 г. «Об электронных сделках и торговле»] // Официальная база законодательства ОАЭ: сайт. — URL: https://elaws.moj.gov.ae/UAE-MOJ_OG/10002S_2006/01-31-2006_0442/UAE-OG_2006-01-30_00001_kait.pdf (дата обращения: 25.03.2025).

139. مرسوم بقانون اتحادي رقم (38) لسنة 2022 بإصدار قانون الإجراءات الجزائية [Федеральный декрет-закон ОАЭ № 38 от 2022 года «Об уголовных мерах»] // Официальная база законодательства ОАЭ: сайт. — URL: https://www.uaelegislation.gov.ae/en/legislations/1609 (дата обращения: 01.04.2025).

140. نظام الإجراءات الجزائية [Положение КСА от 12.06.2013 «Об уголовных мерах»] // Бюро экспертов Совета министров Королевства Саудовская Аравия: сайт. — URL: https://laws.boe.gov.sa/BoeLaws/Laws/LawDetails/8f1b7079-a5f0-425d-b5e0-a9a700f26b2d/1 (дата обращения: 01.04.2025).

141. Указ № 66-156 от 18.02.1386 (хиджра), что соответствует 08.06.1966, включающий в себя измененный и дополненный уголовный закон [الأمر رقم ٦٦-١٥٦ المؤرخ في ١٨ صفر عام ١٣٨٦ الموافق لـ ٨يونيو سنة ١٩٦٦ يتضمن قانون العقوبات المعدل والمتمم] // Поисковая система алжирского права: сайт. — URL: https://legisdz.com/ar/LawTexts/alamr-rqm-66-156-almwrkh-fy-18-sfr-am-1386-almwafq-l8ywnyw-snt-1966-ytdmn-qanwn-alqwbat (дата обращения: 25.01.2025).

142. قانون آیین دادرسی کیفری [Уголовно-процессуальный закон] // Законодательная база ИРИ: сайт. — URL: http://dotic.ir/news/5584/-قانون-آیین-دادرسي-کیفري (дата обращения: 19.03.2025).

143. قانون تجارت الکترونیکی [Закон «Об электронной коммерции»] // Исследовательский центр Исламского совета ИРИ: сайт. — URL: https://rc.majlis.ir/fa/law/show/93997 (дата обращения: 19.03.2025).

144. قرار وزاري رقم ٢٥٩ صادر بتاريخ ٢٧.٠٩.٢٠١٩ في شأن الدليل الإجرائي لتنظيم التقاضي باستخدام الوسائل الالكترونية والاتصال عن بعد في الاجراءات الجزائية [указ министра юстиции ОАЭ № 259 от 27.03.2019 «Относительно процедурного руководства по организации судебного разбирательства с использованием электронных средств и удаленной связи в уголовном судопроизводстве»] // Официальная база законодательства ОАЭ: сайт. — URL: https://elaws.moj.gov.ae/UAE-MOJ_LC-Ar/00_جزائية%20اجراءات/UAE-LC-Ar_2019-03-27_00259_Karwi.html?val=AL1 (дата обращения: 25.03.2025).

145. دليل إجراءات المساعدة القانونية واسترداد الموجودات [Руководство по правовой помощи и процедурам возврата активов] // Министерство внутренних дел Королевства Саудовская Аравия: сайт. — URL: https://www.moi.gov.sa/wps/wcm/connect/dc92bbae-005f-497d-9829-5d8e26d6135f/200.pdf?MOD=AJPERES&CVID=mvFff1Y (дата обращения: 08.04.2025).

146. مرسوم بقانون رقم ٥٤ لسنة ٢٠١٨ بإصدار قانون الخطابات والمعاملات الإلكترونية [Декрет-закон Королевства Бахрейн № 54 2018 года «Об электронных коммуникациях и сделках»] // Электронная база законодательства Королевства Бахрейн: сайт. — URL: https://www.legalaffairs.gov.bh/HTM/L5418.htm (дата обращения: 09.03.2025).

147. مرسوم بقانون اتحادي في شأن مواجهة جرائم غسل الأموال ومكافحة تمويل الإرهاب وتمويل التنظيمات غير المشروعة [Федеральный Декрет-закон ОАЭ № 20 от 2018 г. «О противодействии отмыванию денег и борьбе с финансированием терроризма и деятельности незаконных организаций»] // Законодательная база ОАЭ: сайт. — URL: https://www.uaelegislation.gov.ae/en/legislations/1016?keyword=laundering (дата обращения: 08.04.2025).

148. نظام مكافحة جرائم الإرهاب وتمويله [Положение о борьбе с террористическими преступлениями и его финансированием] // Бюро экспертов Совета министров Королевства Саудовская Аравия: сайт. — URL: https://laws.boe.gov.sa/BoeLaws/Laws/LawDetails/57694209-3eed-46c7-a5d8-a9ed012761d4/1 (дата обращения: 08.04.2025).

149. قانون رقم ٨٠ لسنة٢٠٠٢ بإصدار قانون مكافحة غسل الأموال المعدل بالقانون رقم ٧٨ لسنة ٢٠٠٣ [Закон № 80 от 2002 года о принятии Закона о борьбе с отмыванием денег с поправками, внесенными Законом № 78 от 2003 года] // Центральный банк Арабской Республики Египет: сайт. — URL: https://www.cbe.org.eg/-/media/project/cbe/page-content/rich-text/laws-and-regulations/laws/ar/antimoneylaunderinglaw-ar-other-laws-2.pdf (дата обращения: 08.04.2025).

150. مرسوم بقانون رقم ٤ لسنة ٢٠٠١ بشأن حظر ومكافحة غسل الاموال وتمويل الارهاب [Указ короля Бахрейн № 4 от 2001 г. «Об издании закона о запрещении и борьбе с отмыванием денег и финансировании терроризма»] // Комиссия по законодательству и правовому мнению Королевства Бахрейн: сайт. — URL: https://www.lloc.gov.bh/FullAr/L0401.docx (дата обращения: 08.04.2025).

151. قانون مبارزه با پولشویی [Закон о борьбе с отмыванием денег] // Законодательная база ИРИ: сайт. — URL: https://davoudabadi.ir/page/1896240/-قانون-مبارزه-با-پولشویی (дата обращения: 08.04.2025).

152. قرار مجلس الوزراء رقم (111) لسنة 2022 بشأن تنظيم الأصول الافتراضية ومزودي خدماتها [Решение Совета министров ОАЭ № 111 от 12.12.2022 «Об организации виртуальных активов и поставщиков виртуальных услуг»] // Онлайн база Совета министров ОАЭ: сайт. — URL: https://laws.uaecabinet.ae/ar/materials/law/1623 (дата обращения: 08.04.2025).

153. Law No. 4 of 2022 on Regulating Virtual Assets in the Emirate of Dubai // The Dubai Virtual Assets Regulatory Authority: website. — URL: https://rulebooks.vara.ae/sites/default/files/en_net_file_store/VARA_EN_338_VER1.pdf (accessed 08.04.2025).

154. قرار رئيس مجلس إدارة الهيئة رقم ٢٣ لسنة ٢٠٢٠ م بشأن النظام الخاص بأنشطة الأصول المشفرة [Решение Председателя Совета директоров Управления № 23 от 2020 года о системе деятельности с криптоактивами] // Управление по ценным бумагам и

товарам ОАЭ: сайт. — URL: https://www.sca.gov.ae/Content/Userfiles/Assets/Documents/f79fbf6.pdf (дата обращения: 08.04.2025).

155. قانون الجرائم الإلكترونية رقم ١٧ لسنة ٢٠٢٣ / الجريدة الرسمية. ٢٠٢٣. ١٢/٩. ٢٠٢٣. ص ٣٥٧٩ [Закон № 17 об электронных преступлениях от 2023 г. // Официальный вестник. — 2023. — 2023. — С. 3579].

156. آیین نامه نحوه استفاده از سامانه های رایانه ای یا مخابراتی [Правила использования компьютерных и телекоммуникационных систем] // Официальная база законодательства ИРИ: сайт. — URL: https://rc.majlis.ir/fa/law/show/984023 (дата обращения: 12.04.2025).

157. مرسوم بقانون اتحادي في شأن تنظيم الإعلام [Федеральный декрет-закон «О регулировании медиа»] // Законодательная база ОАЭ: сайт. — URL: https://uaelegislation.gov.ae/ar/legislations/2145 (дата обращения: 02.05.2025)

158. قرار مجلس الوزراء في شأن اللائحة التنفيذية للمرسوم بقانون اتحادي في شأن تنظيم الإعلام [Постановление Совета министров «Исполнительный регламент к Федеральному декрету-закону о регулировании медиа»] // Законодательная база ОАЭ: сайт. — URL: https://uaelegislation.gov.ae/ar/legislations/2547 (дата обращения: 02.05.2025).

159. وزارة النقل والاتصالات وتقنية المعلومات: تعميم رقم ١١ / ٢٠٢٥ السياسة العامة للاستخدام الآمن والأخلاقي لأنظمة الذكاء الاصطناعي أبريل ٢٠٢٥م [Ministry Of Transport, Communications, And Information Technology: Circular 11/2025 The Public Policy For The Safe And Ethical Use Of Artificial Intelligence Systems April 2025] // Qanoon: website. — URL: https://qanoon.om/p/2025/mtcit20259901/ (accessed 20.05.2025).

160. قانون الإجراءات الجنائية رقم 150 لسنة 1950 [Закон АРЕ № 150 от 1950 года «Об уголовных мерах»] // Законодательная база АРЕ: сайт. — URL: https://manshurat.org/node/14676 (дата обращения: 06.05.2025).

161. 刑事訴訟法典 [Уголовно-процессуальный закон] // Законодательная база Макао: сайт. — URL: https://bo.io.gov.mo/bo/i/96/36/codpropencn/codpropen0001.asp#a164 (дата обращения: 06.06.2025).

162. 刑法典 [Уголовный закон] // Законодательная база Макао: сайт. — URL: https://bo.io.gov.mo/bo/i/95/46/codpencn/codpen0001.asp#l2a128 (дата обращения: 06.06.2025).

163. 中华人民共和国刑法 [Уголовное право Китайской Народной Республики] // Национальный конгресс КНР: сайт. — URL: http://www.npc.gov.cn/zgrdw/npc/lfzt/rlys/2008-08/21/content_1882895.htm (дата обращения: 06.06.2025).

164. 本条例旨在综合若干刑事成文法则 [Закон САР Гонконга от 19.11.1971 «О консолидации отдельных уголовных законов» (в ред. от 23.03.2024)] // Законодательная база Гонконга: сайт. — URL:

https://www.elegislation.gov.hk/hk/cap200!en-sc?INDEX_CS=N&xpid=ID_1438402821241_001 (дата обращения: 10.06.2025).

165. 淫褻及不雅物品管制条例 [Закон «О контроле непристойных и неприличных материалов»] // Законодательная база САР Гонконга: сайт. — URL: https://www.elegislation.gov.hk/hk/cap390!en-sc?INDEX_CS=N (дата обращения: 06.06.2025).

166. 电讯条例 [Закон О телекоммуникациях] // Законодательная база САР Гонконга: сайт. — URL: https://www.elegislation.gov.hk/hk/cap106!en-sc?xpid=ID_1438402543810_002&INDEX_CS=N (дата обращения: 06.06.2025).

167. 第 11/2009 號法律. 編號. 2009. № 27. 版數. 971-978 [Закон № 11 о компьютерных преступлениях от 2009 года // Официальный Бюллетень. — 2009. — № 27. — С. 971-978].

168. «2022 年打擊洗錢及恐怖分子資金籌集(修訂)條例草案» [Законопроект о борьбе с отмыванием денег и финансированием терроризма (поправка) 2022 г.] // Законодательный совет Специального административного района Гонконг: сайт. — URL: https://www.legco.gov.hk/tc/legco-business/council/bills.html?bill_key=10015&session=2022 (дата обращения: 06.06.2025).

169. 第 13/2019 號法律 // 公報. 2019. № 25. 版數 1884-1895 [Закон № 13 о сетевой безопасности от 2019 года // Бюллетень. — 2019. — № 25. — С. 1884–1895].

170. 关于办理信息网络犯罪案件适用刑事诉讼程序 [Мнения по некоторым вопросам применения уголовно-процессуальных норм при рассмотрении дел о преступлениях в информационных сетях] // Верховный народный суд КНР: сайт. — URL: https://www.court.gov.cn/fabu-xiangqing-370301.html (дата обращения: 09.03.2025).

171. 最高人民法院 最高人民检察院 关于办理洗钱刑事案件适用法律若干问题的解释 发布时间：2024 年 8 月 19 日 [Объяснение нескольких вопросов применимого законодательства при уголовных делах об отмывании денег Верховным Судом и Верховной Народной Прокуратурой от 19.08.2024] // Верховная Народная Прокуратура КНР: официальный сайт. — URL: https://www.spp.gov.cn/xwfbh/wsfbt/202408/t20240819_663652.shtml#2 (дата обращения: 21.04.2025).

172. 中华人民共和国国务院令 政务数据共享条例 [Приказ Государственного совета Китайской Народной Республики «Положение о предоставлении правительственных данных»] // Правительство КНР: сайт. — URL: https://www.gov.cn/zhengce/content/202506/content_7026294.htm (дата обращения: 12.06.2025).

173. 最高检印发《人民检察院办理网络犯罪案件规定》 [Уведомление Высшей народной прокуратуры КНР «Об издании положений касательно сетевых преступлений, расследуемых народной прокуратурой»] // Высшая народная

прокуратура КНР: сайт. — URL: https://www.spp.gov.cn/spp/xwfbh/wsfbh/202101/t20210125_507446.shtml (дата обращения: 25.03.2025).

174. 生成式人工智能服务管理暂行办法 [Временные меры по управлению услугами искусственного интеллекта поколений] // Управление КНР по киберпространству: сайт. — URL: https://www.cac.gov.cn/2023-07/13/c_1690898327029107.htm (дата обращения: 29.09.2024).

175. 生成式人工智能服务管理办法 [О глубоком синтезе в информационных услугах на основе Интернета] // Управление КНР по киберпространству: сайт. — URL: https://www.cac.gov.cn/2023-04/11/c_1682854275475410.htm (дата обращения: 29.09.2024).

176. 互联网信息服务算法推荐管理规定 [Об алгоритмах рекомендаций в информационных услугах на основе Интернета] // Государственный совет Китайской Народной Республики: сайт. — URL: https://www.gov.cn/zhengce/zhengceku/2022-01/04/content_5666429.htm (дата обращения: 29.09.2024).

177. 中华人民共和国刑事诉讼法 [Уголовно-процессуальный закон Китайской Народной Республики] // Портал центрального правительства. Законы и нормативные акты: сайт. — URL: https://www.gov.cn/flfg/2012-03/17/content_2094354.htm (Дата обращения: 21.10.2024).

178. 人民检察院刑事诉讼规则 [Уголовно-процессуальные правила Верховной Народной прокуратуры от 30.12.2019] // Онлайн-законодательство Верховной народной прокуратуры: сайт. — URL: https://www.spp.gov.cn/spp/xwfbh/wsfbh/201912/t20191230_451490.shtml#1 (дата обращения: 21.10.2024).

179. 公安机关办理刑事案件电子数据取证规则 [Правила сбора электронных данных для органов общественной безопасности для рассмотрения уголовных дел] // Бюро общественной безопасности Чунцина. URL: https://gaj.cq.gov.cn/zslm_245/wlaqgl/flfg/201912/t20191221_2043591.html (дата обращения: 20.03.2025).

180. 中华人民共和国反洗钱法 [Закон о борьбе с отмыванием денег Китайской Народной Республики] // Правительство КНР: официальный сайт. — URL: https://www.gov.cn/yaowen/liebiao/202411/content_6985765.htm (дата обращения: 21.04.2025).

181. ማብራሪያ የኮምፒውተር ወንጀል አዋጅ [Разъяснение Закона о компьютерных преступлениях] // Законодательная база ФДРЭ: сайт. — URL: https://www.lawethiopia.com/images/draft%20laws/Computer%20Crime%20-%20Explanatory%20note%20final%202.pdf (дата обращения: 10.03.2025).

Руководящие документы и отчёты государственных органов

182. Abu Dhabi Government Digital Strategy 2025-2027 // Abu Dhabi Media Office: website. — URL: https://www.mediaoffice.abudhabi/en/topic/abu-dhabi-government-digital-strategy-2025-2027/ (accessed 25.03.2025).

183. Assessing India's Cybersecurity Regulations in a Dynamic Environment // DSCI: website. — URL: https://www.dsci.in/files/content/knowledge-centre/2024/Assessing-India-Cybersecurity-Regulations-DSCI-SAP.pdf (accessed 24.05.2025).

184. Digital Participation Strategy // U.ae: website. — URL: https://u.ae/en/about-the-uae/digital-uae/digital-inclusion/national-digital-participation-strategy (accessed 20.08.2023).

185. Dubai Autonomous Transportation Strategy // U.ae: website. — URL: https://u.ae/en/about-the-uae/strategies-initiatives-and-awards/strategies-plans-and-visions/transport-and-infrastructure/dubai-autonomous-transportation-strategy (accessed 25.03.2025).

186. Dubai Blockchain Strategy // Digital Dubai. URL: https://www.digitaldubai.ae/initiatives/blockchain (accessed 20.08.2023).

187. Dubai Data Strategy // U.ae: website. — URL: https://u.ae/en/about-the-uae/strategies-initiatives-and-awards/strategies-plans-and-visions/government-services-and-digital-transformation/dubai-data-strategy (accessed 25.03.2025).

188. Dubai eCommerce strategy // U.ae: website. — URL: https://u.ae/en/about-the-uae/strategies-initiatives-and-awards/strategies-plans-and-visions/government-services-and-digital-transformation/dubai-e-commerce-strategy (accessed 25.03.2025).

189. Dubai Internet of Things Strategy // U.ae: website. — URL: https://u.ae/en/about-the-uae/strategies-initiatives-and-awards/strategies-plans-and-visions/strategies-plans-and-visions-untill-2021/dubai-internet-of-things-strategy (accessed 25.03.2025).

190. Dubai Paperless Strategy // Digital Dubai: website. — URL: https://www.digitaldubai.ae/initiatives/paperless (accessed 25.03.2025).

191. Dubai 3D Printing Strategy // U.ae. URL: https://u.ae/en/about-the-uae/strategies-initiatives-and-awards/strategies-plans-and-visions/industry-science-and-technology/dubai-3d-printing-strategy (accessed 25.03.2025).

192. National Strategy for Advanced Innovation // U.ae: website. — URL: https://u.ae/en/about-the-uae/strategies-initiatives-and-awards/strategies-plans-and-visions/innovation-and-future-shaping/national-strategy-for-advanced-innovation (accessed 25.03.2025).

193. National Policy for Quality of Digital Life // U.ae. URL: https://u.ae/en/about-the-uae/strategies-initiatives-and-awards/policies/government-services-and-digital-transformation/national-policy-for-quality-of-digital-life (accessed25.03.2025).

194. Policies, strategies and guidelines // Omanuna: website. — URL: https://oman.om/en/policies-strategies-and-guidlines (accessed 25.03.2025).

195. Qatar National Cyber Security Strategy. May 2014 // The George Washington University: website. — URL: https://nsarchive.gwu.edu/sites/default/files/documents/3903662/Qatari-Government-Qatar-National-Cyber-Security.pdf (дата обращения: 25.03.2025).

196. Smart Dubai 2021 Strategy // U.ae. URL: https://u.ae/en/about-the-uae/strategies-initiatives-and-awards/strategies-plans-and-visions/strategies-plans-and-visions-untill-2021/smart-dubai-2021-strategy (accessed 20.08.2023).

197. the Dubai Cyber Security Strategy — Updated // U.ae: website. — URL: https://u.ae/en/about-the-uae/strategies-initiatives-and-awards/strategies-plans-and-visions/government-services-and-digital-transformation/dubai-cyber-security-strategy (дата обращения: 25.03.2025).

198. The Federal Democratic Republic of Ethiopia. National Cyber Security Policy and Strategy. 2021 // INSA: website. — URL: https://insa.gov.et/documents/20124/0/National+Cyber+security+Policy%26+StrategyFDRE.docx/03b2d42e-5cb3-f29e-f8f8-fe4ad3d94586?t=1639143692057&download=true (дата обращения: 25.03.2025).

199. The UAE Digital Government Strategy 2025 // U.ae: website. — URL: https://u.ae/en/about-the-uae/strategies-initiatives-and-awards/strategies-plans-and-visions/government-services-and-digital-transformation/uae-national-digital-government-strategy (дата обращения: 25.03.2025).

200. الإطار القانوني الاسترشادي [Руководящая правовая база] // Портал Совета сотрудничества арабских государств Персидского залива: сайт. — URL: http://www.gcc-egov.org/web/guest/laws;jsessionid=B5AC15C1BAC7D86B98BCC5A668E5D826 (дата обращения: 25.03.2025).

201. الضوابط والإرشادات [Контроль и руководящие принципы] // Национальное управление кибербезопасности KCA: сайт. — URL: https://nca.gov.sa/legislation (дата обращения: 16.04.2023), الأمن السيبراني في قطاع الاتصالات والفضاء والتقنية [Кибербезопасность в телекоммуникационном, космическом и технологическом секторе] // Комиссия по связи, космосу и технологиям KCA: сайт. — URL: https://www.cst.gov.sa/ar/RulesandSystems/CyberSecurity/Pages/default.aspx (дата обращения: 16.04.2023).

202. المحافظة على خصوصية البيانات الشخصية [Поддержание конфиденциальности персональных данных] // Комиссия по связи, космосу и технологиям KCA: сайт. — URL: https://www.cst.gov.sa/ar/RulesandSystems/privacy/Pages/default.aspx (дата обращения: 16.04.2023).

203. حوكمة تقنية المعلومات [Управление информационными технологиями] // Министерство транспорта, коммуникаций и информационных технологий Султаната Оман: сайт. — URL:

https://www.ita.gov.om/ITAPortal_AR/Pages/Page.aspx?NID=2187&PID=6706&LID=247 (дата обращения: 13.07.2023).

204. المعايير والسياسات [Стандарты и политика] // Центр электронной безопасности в Дубай: сайт. — URL: https://www.desc.gov.ae/ar/regulations-ar/standards-policies-ar/ (дата обращения: 17.07.2023).

205. سياسات حوكمة البيانات الوطنية [Национальная политика управления данными] // Управление KCA по данным и искусственному интеллекту: сайт. — URL: https://sdaia.gov.sa/en/SDAIA/about/Documents/Policies005.pdf (дата обращения: 25.03.2025).

206. استراتيجية الإمارات الوطنية للذكاء الاصطناعي [Национальная стратегия ОАЭ по искусственному интеллекту 2031] // Министерство ОАЭ по искусственному интеллекту, цифровой экономике и удалённой работе: сайт. — URL: https://ai.gov.ae/wp-content/uploads/2021/07/UAE-National-Strategy-for-Artificial-Intelligence-2031-AR.pdf (дата обращения: 25.03.2025).

207. البرنامج الوطني للاقتصاد الرقمي [Национальная программа цифровой экономики] // Министерство транспорта, связи и информационных технологий Султаната Оман: сайт. — URL: https://ita.gov.om/ITAPortal_AR/Our_Projects/Our_Projects_List.aspx?svc=657&NID=170001&Odt=37 (дата обращения: 25.03.2025) и البرنامج الوطني للذكاء الاصطناعي والتقنيات المتقدمة [Национальная программа искусственного интеллекта и передовых технологий] // Министерство транспорта, связи и информационных технологий Султаната Оман: сайт. — URL: https://mtcit.gov.om/ITAPortal_AR/Our_Projects/Our_Projects_List.aspx?svc=657&NID=170035&Odt=37 (дата обращения: 25.03.2025).

208. الاستراتيجية الوطنية للأمن السيبراني لدولة الكويت ٢٠١٧-٢٠٢٠ [Национальная стратегия Государства Кувейт по кибербезопасности 2017–2020 гг.] // Управление по регулированию коммуникаций и информационных технологий Государства Кувейт: сайт. — URL: https://citra.gov.kw/sites/ar/LegalReferences/Cyber%20Security.pdf (дата обращения: 09.03.2025).

209. الإستراتجية الوطنية الأمن السيبراني ٢٠٢٤-٢٠٣٠ دولة قطر [Национальная стратегия кибербезопасности 2024–2030 г. Государство Катар] // Национальное управление кибербезопасности Государства Катар: сайт. — URL: https://ncsa.gov.qa/sites/default/files/2024-09/StrategyM9%20-%20AR%20OL_0.pdf?csrt=5654088632520333724 (дата обращения: 05.04.2025).

210. الاستراتيجية الوطنية للأمن السيبراني [Национальная стратегия кибербезопасности] // Национальное управление кибербезопасности KCA: сайт. — URL: https://nca.gov.sa/strategic (дата обращения: 25.03.2025).

211. الاستراتيجية الوطنية للأمن السيبراني [Национальная стратегия кибербезопасности] // Национальный центр кибербезопасности Королевства Бахрейн: сайт. — URL: https://www.ncsc.gov.bh/ar/national-strategy.html (дата обращения: 11.07.2023).

212. الاستراتيجية الوطنية للأمن السيبراني [Национальная стратегия кибербезопасности] // Управление по регулированию телекоммуникаций и цифрового государства ОАЭ: сайт. — URL: https://tdra.gov.ae/ar/national-cybersecurity-strategy (дата обращения: 25.03.2025).

213. البرنامج الوطني للاقتصاد الرقمي [Национальная программа цифровой экономики] // Министерство транспорта, связи и информационных технологий Султаната Оман: сайт. — URL: https://ita.gov.om/ITAPortal_AR/Our_Projects/Our_Projects_List.aspx?svc=657&NID=170001&Odt=37 (дата обращения: 05.04.2025).

214. البرنامج الوطني للذكاء الاصطناعي والتقنيات المتقدمة [Национальная программа искусственного интеллекта и передовых технологий] // Министерство транспорта, связи и информационных технологий Султаната Оман: сайт. — URL: https://mtcit.gov.om/ITAPortal_AR/Our_Projects/Our_Projects_List.aspx?svc=657&NID=170035&Odt=37 (дата обращения: 05.04.2025).

215. طرح کلان و معماری شبکه ملی اطلاعات [Генеральный план и архитектура национальной информационной сети] // Законодательная база ИРИ: сайт. — URL: https://davoudabadi.ir/page/60451726 (дата обращения: 04.05.2025).

216. پیشگیری و مقابله با قمار در فضای مجازی [Предотвращение и борьба с азартными играми в киберпространстве] // Законодательная база ИРИ: сайт. — URL: https://davoudabadi.ir/page/1790426 (дата обращения: 04.05.2025).

217. سند ملی هوش مصنوعی جمهوری اسلامی ایران [Национальный документ Исламской Республики Иран по искусственному интеллекту] // Законодательная база ИРИ: сайт. — URL: https://davoudabadi.ir/page/0392571/سند-ملی-هوش-مصنوعی-جمهوری-اسلامی-ایران (дата обращения: 04.05.2025).

218. استا تيجية قطر الوطنية في نجال الذكاء الاصطناعي [Стратегия Государства Катар в области искусственного интеллекта] // Министерство связи и информационных технологий Государства Катар: сайт. — URL: https://mcit.gov.qa/sites/default/files/strtyjy_qtr_lwtny_fy_mjl_ldhk_lstny.pdf (дата обращения: 25.03.2025).

219. استراتيجية الحكومة الإلكترونية لدولة قتر ٢٠٢٠ [Стратегия электронного правительства Государства Катар 2020] // Министерство связи и информационных технологий Государства Катар: сайт. — URL: https://mcit.gov.qa/sites/default/files/qatar-e-government-2020-strategy-ar_0.pdf (дата обращения: 25.03.2025).

220. Мишааль Абдулла бин Хусейн. تقرير مركز الإستجابة لطوارئ الحاسب الآلي لجرائم تقنية المعلومات ٢٠٠٨-٢٠٠٩ [Специальный Доклад Центра реагирования на компьютерные инциденты по преступлениям в области информационных технологий 2008-2009 гг.] // Официальная онлайн база законодательства ОАЭ: сайт. — URL: https://elaws.moj.gov.ae/UAE-MOJ_Fokeh/15_الرابع%20العدد/UAE-MOJ_تقرير%20مركز%20الإستجابة%20لطوارئ%20الحاسب%20الآلي%20لجرائم%20تقنية%20المعلومات.html?val=UAE-FokehAA1 (дата обращения: 18.03.2025).

Отечественные монографии, научные и учебные издания

221. Адрианов А.К. Арабские монархии Персидского залива — новый технологический полюс?: аналитические тезисы № 6 / 2025. — Москва: Центр Примакова, 2025. — 36 с.

222. Балил ‘Абд ал-Карим. Терминология Корана: лингвистический и семантический анализ / пер. с англ. С. М. Коваленко. — Санкт-Петербург: Петербургское востоковедение, 2022. — 216 с. ISBN 978-5-85803-585-5.

223. Васюков В.Ф. Преступления в сфере высоких технологий и информационной безопасности: учебное пособие / В.Ф. Васюков, А.Г. Волеводз, М.М. Долгиева, В.Н. Чаплыгина; под науч. ред. А.Г. Волеводза. — Москва: Прометей, 2023. — 1086 с. ISBN 978-5-00172-447-6.

224. Васюков В.Ф. Противодействие преступлениям в сфере незаконного оборота наркотиков, совершаемым с использованием информационно-телекоммуникационных технологий: учеб. пособие / В.Ф. Васюков, К.К. Клевцов, В.И. Малик; под науч. ред. А.Г. Волеводза. — Москва: Прометей, 2023. — 468 с. ISBN 978-5-00172-523-7.

225. Васюков В.Ф. Теоретические и правовые аспекты расследования преступлений с использованием абонентской информации: монография / Под ред. докт. юрид. наук А.Г. Волеводза. — Орел: Издательство «Картуш», 2020. — 339 с.

226. Волеводз А.Г. Международные правоохранительные организации. — Москва: Издательство Проспект, 2011. — 344 с. ISBN 978-5-392-02595-4

227. Волеводз А.Г. Международные правоохранительные организации: Учебное пособие в 5-ти частях / А. Г. Волеводз. — Москва: ООО «Издательство Прометей», 2023. — 224 с. (Библиотека магистратуры «Международное сотрудничество в сфере правоохранительной деятельности и уголовной юстиции»; Часть II; Судебные и юридические сети). ISBN 978-5-00172-515-2.

228. Волеводз А.Г. Противодействие компьютерным преступлениям: правовые основы международного сотрудничества. — Москва: ООО Издательство «Юрлитинформ», 2002. — 496 с. ISBN 5-93295-041-2.

229. Завадская Е.П. Амхарский язык. Общественно-политический перевод / Е.П. Завадская. — Москва: МГИМО-Университет, 2011. — 345 с. ISBN 978-5-9228-0671-8.

230. Индонезийский язык для международников = Bahasa Indonesia untuk hubungan internasional. Учебник / под ред. Н.А.Толмачёв. — Москва: МГИМО-Университет, 2014. — 291 с. ISBN 978-5-9228-1084-5.

231. Клевцов К. К. Передача уголовного преследования (уголовного судопроизводства) / К. К. Клевцов, А. Г. Волеводз. — Москва: ООО «Издательство Прометей», 2022. — 762 с. ISBN 978-5-00172-360-8.

232. Криминалистика: учебник / А. В. Гриненко, В. А. Дударев, С. С. Маевский. Москва: ООО «Проспект», 2025. 432 с. ISBN 978-5-39240-931-0.

233. Колычева А.Н., Васюков В.Ф. Расследование преступлений с использованием компьютерной информации из сети Интернет: учебное пособие / под ред. А. Г. Волеводза. — Москва: Проспект, 2020. — 200 с. ISBN 978-5-39231-742-4.

234. Малиновский А. А. История и методология юридической науки. — Москва: ООО «Издательство Прометей», 2022. — 562 с. ISBN 978-5-00172-277-9.

235. Малиновский А. А. Сравнительное уголовное право: учебник. 2-ое издание дополненное и переработанное. — Москва: Издательство «Юрлитинформ», 2016. — 592 с.

236. Международное уголовное право: Учебное пособие для специалистов, профессионально занимающихся проблемами борьбы с преступностью / А. Ю. Скуратова, И. И. Синякин. — Москва: ООО «Проспект», 2025. — 560 с.

237. Международное управление Интернетом / Е. С. Зиновьева, А. А. Игнатов, А. А. Уланов [и др.]. — Москва: Серпантин Про (ИП Гончаров А.В.), 2025. — 186 с. ISBN 978-5-6053935-0-4

238. Правовая экспертиза / В. В. Дубровин, А. Г. Волеводз, Е. Г. Дубровина [и др.]. — Москва: МГИМО, 2024. — 364 с. ISBN 978-5-9228-2898-7.

239. Противодействие криптовалютным преступлениям в зарубежных странах / В. Ф. Васюков, А. Г. Волеводз, К. К. Клевцов [и др.]. — Москва: ООО Издательский дом «Юрлитинформ», 2025. — 504 с.

240. Рубинчик Ю.А. Грамматика современного персидского литературного языка / под ред. М.И. Карповой. — Москва: Восточная литература РАН, 2001. — 600 с. ISBN 5-02-018177-3.

241. Сидоренко Э. Л. Криптовалюта и будущее цифровых финансов. — Москва: МГИМО МИД России, 2023. — 36 с.

242. Сидоренко Э.Л. Право цифровых активов: учебник для бизнеса. — Москва: Издательский дом «Юрлитинформ», 2025. — 312 с. ISBN 978-5-6053178-2-1.

243. Себякин А.Г. Тактика использования знаний в области компьютерной техники: монография. — Москва: Юрлитинформ, 2023. — 181 с. ISBN 978-5-4396-2465-2.

244. Стельмах В.Ю. Производство следственных действий, направленных на получение и использование компьютерной информации: монография / В.Ю. Стельмах, О.М. Ефремова, В.Ф. Васюков / под общ. ред. А. Г. Волеводза. — Москва: Проспект, 2021. — 480 с. ISBN 978-5-392-33469-8.

245. Сюкияйнен Л. Р. Исламское право и диалог культур в современном мире. 2-ое издание, переработанное. — Москва: НИУ «Высшая школа экономики», 2025. — 680 с. I

246. Татаринов М. К. Уголовная юрисдикция в международном уголовном праве. — Москва: ООО «Издательство Прометей», 2023. — 828 с. ISBN 978-5-00172-449-0.

247. Уголовный процесс: учебник и практикум. 9-е издание, переработанное и дополненное. — Москва: Издательство Юрайт, 2024. — 361 с. ISBN 978-5-534-16310-0

248. Цифровое право: учебник / под ред. Э.Л. Сидоренко. — Москва: Юрлитинформ, 2024. — 720 с. ISBN 978-5-4396-2619-9.

249. Яковенко Э.В. Арабский язык. Практический курс перевода: учебное пособие / Э.В. Яковенко. — Москва: Издательство восточной литературы, 2019. — 464 с. ISBN 978-5-6041860-6-0.

250. Яковенко Э.В. Арабский язык для юристов-международников. Часть 1: Учебник / под ред. А.А. Малиновского, Н.М. Шуйской. — Москва: Прометей, 2025. — 392 с. ISBN 978-5-00172-711-8.

251. Collecting Electronic Evidence in Criminal Cases in Russia and Foreign Countries: Experiences and Problems: Monograph / editors S.P. Shcherba (Russian ed.) and P.A. Litvishko (English ed.). — Moscow: Publishing House “Gorodets”, 2024. — 224 p. ISBN 978-5-907762-35-0.

Зарубежные монографии, научные и учебные издания

252. Ахмад Хамао, Ала Аваад, Вала Абдулла. Электронные доказательства (юридические и технические аспекты). — Палестина: Юридический институт Бирзейтского университета, 2015 (на араб. яз.).

253. Мохаммад Сулейман, Салах Газаль, Винсент Карчеди, Адель Аль-Адави. Метавселенная: возможности и проблемы безопасности. — Эр-Рияд: Издательский дом университета Наифа, 2023. — 114 с. [محمد سليمان، صلاح غزال، فنسنت كارشيدي، عادل العدوي. الميتافيرس: الفرص والتحديات الأمنية. دار جامعة نايف للنشر، ٢٠٢٣. ١١٤ ص.].

254. 'Abd al-Rahmān b. Nasr al-Shayzarī. The Book of the Islamic Market Inspector. — Oxford University Press, 2004. — 224 p.

255. Cho J., Tom Dieck M.C., Jung T. What is the Metaverse? Challenges, Opportunities, Definition, and Future Research Directions. In Extended Reality and Metaverse - Immersive Technology in Times of Crisis / ed. M.C.Tom Dieck, T. Jung, S. Loureiro. — Heidelberg: Springer, 2023.

256. Cyber Crime Investigation Manual. DSCI, 2011. 137 p. — URL: https://jhpolice.gov.in/sites/default/files/documents-reports/jhpolice_cyber_crime_investigation_manual.pdf (accessed 08.04.2025).

257. El-Kady R. Artificial Intelligence from the Criminal Law Perspective. Proceedings of the 10th International Conference on Advanced Intelligent Systems and Informatics 2024. — Springer Nature, 2025. — P. 162–173.

258. El-Kady R. Unmasking Virtual Crimes: Investigating and Proving Evidence in the Metaverse. In Unveiling Social Dynamics and Community Interaction in the Metaverse. — IGI Global, 2025. — P. 389–444.

259. El-Kady R. Artificial intelligence and criminal law. In: Artificial Intelligence Approaches to Sustainable Accounting / ed. M. Tavares, G. Azevedo, J. Vale, R. Marques, M. Bastos. — IGI Global, 2024. — P. 34–52.

260. El-Kady R. Investigating forensic evidence in metaverse: a comparative analytical study. In Forecasting Cyber Crimes in the Age of the Metaverse / ed. H. Elshenraki. — IGI Global, 2024. — P. 227–258.

261. El-Kady R. Navigating the legal maze: electric self-driving cars and the complexities of criminal law. Solving Fundamental Challenges of Electric Vehicles / ed. M. Shaik. — IGI Global, 2024. — P. 215–247.

262. Hakmeh J. Cybercrime and the Digital Economy in the GCC Countries / J. Hakmeh. — London: Chatham House, 2017.

263. Huddleston B. Digital cocaine: A journey toward iBalance. — Christian Art Publishers, 2016.

264. Geschonneck A. Computer-Forensik. Computerstraftaten erkennen, ermitteln, aufklären. 5. aktualisierte und erweiterte Auflage. Heidelberg: dpunkt Verlag, 2011.

265. Global Fraud Summit. — Tokyo: National Police Agency of Japan, 2024.

266. Kamali M. H. Principles of Islamic jurisprudence (Ushul al-Fiqh). — Cambridge: Islamic Texts Society, 1991.

267. Kamali M.N. Maqasid al-Shariah made simple. — International Institute of Islamic Thought, 2008. — 32 p.

268. Kamali M.N. The principles of Islamic jurisprudence. — Cambridge Scholars Publishing, 2018. — 550 p.

269. Kardaras N. Glow kids: How screen addiction is hijacking our kids - and how to break the trance. — St. Martin’s Griffin, 2017. — 288 p.

270. Nirmala G.K., Ato Serkaddis Zegeye. Criminal law I. Teaching material. Justice and Legal System Research Institute, 2009. 286 p. — URL: https://www.lawethiopia.com/images/teaching_materials/Criminal%20law%20I.pdf (accessed 25.03.2025).

271. Pemberian Keterangan Saksi Lewat Videoconference Dalam Rancangan KUHAP. — Jakarta: Institute for Criminal Justice Reform, 2015.

272. Przeworski A., Teune H. The Logic of Comparative Social Inquiry. — Wiley-Interscience, 1970. — 153 p.

273. Ragin C.C. The Comparative Method: Moving Beyond Qualitative and Quantitative Strategies. — Berkeley: University of California Press, 1989. — 218 p.

274. The Ministry of Defense of the Republic of Indonesia. A Road Map to Cyber Defense National Strategy. — Jakarta: The Ministry of Defense of the Republic of Indonesia, 2013.

275. UNODC. Casinos, Money Laundering, Underground Banking and Transnational Organized Crime in East and Southeast Asia. — Vienna: UNODC, 2024.

276. UNODC. Transnational Organized Crime and the Convergence of Cyber-Enabled Fraud, Underground Banking and Technological Innovation in Southeast Asia: A Shifting Threat Landscape. Vienna: UNODC, 2024.

277. العملات المشفرة [Зашифрованные валюты] // Центральный банк Иордании: сайт. — URL: https://www.cbj.gov.jo/EchoBusV3.0/SystemAssets/8f23f11e-de4c-4538-91f7-82aab2d7bf04.pdf (дата обращения: 08.04.2025).

278. عبدالرزاق المرجان ، محمد شوقي ، يوسف السبعاوي ، محمد المنشاوي ، سيوكي لي ، جلال الهاشل. الدليل الاسترشادي للتعامل مع الأدلة الجنائية الرقمية في الدول العربية. دار جامعة نايف للنشر، ٢٠٢٤. ٦٤ ص. [Аль-Марджан А.Р., Шаки М., Аль-Сабави Ю., Аль-Маншави М., Ли С., Аль-Хашель Дж. Руководство по работе с цифровыми судебно-медицинскими доказательствами в арабских странах. — Издательский дом Университета Наиф, 2024. — 64 с.].

279. نضال أدلبي، بحث بعنوان تطوير وتنسيق التشريعات السيبرانية في المنطقة العربية ومواجهة الجرائم السيبرانية، الأمم المتحدة ، الإسكوا،نقل بتصرف، ص 14- 18 [Нидаль Эдби. Разработка и гармонизация киберзаконодательства в арабском регионе и противостояние киберпреступности. — ЭСКЗА ООН. — С. 14–18].

280. حماية الفضاء الإلكتروني في دول مجلس التعاون لدول الخليج العربية ريتشارد كلارك, روبرت نيك. [Нир Р., Кларк Р. Защита электронного пространства в странах Совета сотрудничества стран Арабского залива]. Emirates Center for Strategic Studies and Research, 2011. 55 с. — URL: https://www.ecssr.ae/wp-content/uploads/2019/01/ELS_AR_140.pdf (дата обращения: 25.03.2025).

281. ليلى الجنابي. فعالية القوانين الوطنية والدولية في مكافحة الجرائم السيبرانية [Лайла Аль-Джанаби. Эффективность национального и международного права в борьбе с киберпреступлениями] // Центр светских работ и исследований в арабском мире: сайт. — URL: https://www.ssrcaw.org/ar/show.art.asp?aid=571423 (дата обращения: 25.03.2025).

282. الجريمة الإلكترونية في المجتمع الخليجي وكيفية مواجهتها [Электронные преступления в обществе Залива и как им противостоять]. Эр-Рияд: Генеральный секретариат Совета сотрудничества арабских государств Персидского залива, 2016. 208 с. — URL: https://www.gcc-sg.org/ar-sa/CognitiveSources/DigitalLibrary/Lists/DigitalLibrary/البحوث%20الأمنية/كتاب%20الجريمة%20الالكترونية%20سلطنة%20عمان.pdf (дата обращения: 25.03.2025).

283. سلطان الجمال، حميد البناي. مكافحة جرائم الاتجار بالبشر عبر شبكات التواصل الاجتماعي: دراسة استشرافية لسبل مكافحة الاتجار بالبشر من واقع قضايا الاتجار بالبشر بإمارة دبي. المكتب العربي للشؤون الأمنية والإعلامية العربية التابع لمجلس وزراء الداخلية العرب بجامعة الدول العربية، ٢٠٢١. ٤٠ ص [Аль-Джамал С., Аль-Баннаи Х. Борьба с преступлениями, связанными с торговлей людьми,

через социальные сети: перспективное исследование способов борьбы с торговлей людьми на основе случаев торговли людьми в эмирате Дубай. — Арабское бюро по вопросам безопасности и СМИ Совета арабских министров внутреннил дел Лиги арабских государств, 2021. — 40 с.]. URL: https://www.aimc-hr.org/mcms-store/pdf/886eddbd-7484-419c-a26d-e097f02e2a2c.pdf (дата обращения: 10.05.2025).

284. عمر محمد بن يونس. المخدرات والمؤثرات العقلية عبر الإنترنت. الإسكندرية: دارالفكر الجامعى، ٢٠٠٤. ١٤٩ ص. [Омар Мохаммед бин Юнис. Онлайн-наркотики и психотропные вещества. — Александрия: Университетский дом аль-фикр, 2004. — 149 с].

285. أبو دوح خالد. المخدرات الرقمية: مقاربة للفهم. الندوة العلمية" المخدرات وتأثيرها على الشباب. الرياض: جامعة نايف العربية للعلوم الأمنية. ١٢-١٨.٠٢.٢٠١٦ [Абу Дух Х. Цифровые наркотики: Подход к пониманию. Научный симпозиум «Наркотики и их влияние на молодежь». — Эр-Рияд: Наифский арабский университет наук безопасности. 12–18.02.2016].

286. إناء فتيح على الرفاعي، خورج النسرين جورج عيسى زينة. المخدرات الرقمية" أنواعها والإدمان على مسببها. بيروت: المركز العربي للبحوث القانونية والقضائية، ٢٠٢٢. ١٢٨ ص. [Хордж ан-Насрин Джордж Исса Зейна, Ваза Фатиха ибн аль-Рифаи. Цифровые наркотики, их виды и причины зависимости. — Бейрут: Арабский центр правовых и судебных исследований, 2022. — 128 с.].

Диссертации и авторефераты диссертаций

287. Агибалов В.Ю. Виртуальные следы в криминалистике и уголовном процессе: автореф. дис. ... канд. юрид. наук: 12.00.09 / Агибалов Владимир Юрьевич. Воронеж, 2010. 24 с.

288. Асламова В.С. Оперативно-розыскное противодействие преступлениям, совершаемым в сфере незаконного оборота наркотиков с использованием сети «Интернет» на территории Российской Федерации и Республики Казахстан (сравнительно-правовое исследование): дис. ... канд. юрид. наук: 5.1.4. / Асламова Валентина Сергеевна. Санкт-Петербург, 2024. 168 с.

289. Атаманов Р.С. Основы методики расследования мошенничества в сети Интернет: дис. ... канд. юрид. наук: 12.00.09 / Атаманов Руслан Сергеевич. Москва, 2012. 182 с.

290. Бошаева Л.Л. Предупреждение киберпреступности в отношении несовершеннолетних: дис. ... канд. юрид. наук: 5.1.4. / Бошаева Лариса Лангиевна; Москва, 2025. 259 с.

291. Вражнов А.С. Криминалистический риск при расследовании неправомерного доступа к компьютерной информации: дис. ... канд. юрид. наук: 12.00.12 / Вражнов Алексей Сергеевич. Москва, 2015. 218 с.

292. Гайфутдинов Р.Р. Понятие и квалификация преступлений против безопасности компьютерной информации: дис. ... канд. юрид. наук: 12.00.08 / Гайфутдинов Рамиль Рустамович. Казань, 2017. 243 с.

293. Григорян Г.Р. Мошенничество в сфере компьютерной информации: проблемы криминализации, законодательной регламентации и квалификации: дис. ... канд. юрид. наук: 12.00.08 / Григорян Гарик Рафикович. Самара, 2021. 243 с.

294. Давыдов В.О. Информационное обеспечение раскрытия и расследования преступлений экстремистской направленности, совершенных с использованием компьютерных сетей: дис. ... канд. юрид. наук: 12.00.12 / Давыдов Владимир Олегович. Тула, 2013. 264 с.

295. Долгиева М. М. Теоретические основания уголовной политики в сфере оборота криптовалюты: дис. ... док. юрид. наук / Долгиева Мадина Муссаевна. Москва, 2023. 474 с.

296. Дрога А.А. Развитие методики судебно-бухгалтерских экспертиз на основе данных, сопряженных с использованием компьютерных средств: дис. ... канд. юрид. наук: 12.00.12 / Дрога Анастасия Александровна. Москва, 2019. 253 с.

297. Евдокимов К.Н. Противодействие компьютерной преступности: теория, законодательство, практика: дис. ... док. юрид. наук: 12.00.08 / Евдокимов Константин Николаевич. Москва, 2022. 557 с.

298. Ефремова О.М. Реализация полномочий следователя, направленных на получение и использование компьютерной информации при производстве следственных действий: дис. ... канд. юрид. наук: 12.00.09 / Ефремова Ольга Михайловна. Орел, 2021. 225 с.

299. Жаворонков В.А. Информационно-компьютерное обеспечение судебной экспертизы маркировочных обозначений транспортных средств: дис. ... канд. юрид. наук: 12.00.12 / Жаворонков Владимир Алексеевич. Москва, 2020. 268 с.

300. Завьялова Д.В. Расследование преступлений в сфере компьютерной информации: отечественный и зарубежный опыт: дис. ... канд. юрид. наук: 12.00.12 / Завьялова Дарья Владимировна. Москва, 2022. 242 с.

301. Зиновьева Н.С. Компьютерная информация, преобразованная методами криптографии, в раскрытии и расследовании преступлений: дис. ... канд. юрид. наук: 12.00.12 / Зиновьева Нина Сергеевна. Краснодар, 2021. 207 с.

302. Ильницкий А.С. Противодействие криминальной идеологии в сети Интернет: дис. ... канд. юрид. наук: 5.1.4. / Ильницкий Александр Сергеевич. Краснодар, 2022. 213 с.

303. Камко А.С. Предупреждение мошенничества с использованием телекоммуникационных и компьютерных сетей: дис. ... канд. юрид. наук: 12.00.08 / Камко Артем Сергеевич. Владивосток, 2020. 228 с.

304. Кананович А.И. Уголовно-правовая защита авторских прав в глобальной сети Интернет (на примере законодательств России и Франции): дис. ... канд. юрид. наук: 12.00.08 / Кананович Анастасия Игоревна. Москва, 2013. 229 с.

305. Коломинов В.В. Расследование мошенничества в сфере компьютерной информации: научно-теоретическая основа и прикладные аспекты первоначального этапа: дис. ... канд. юрид. наук: 12.00.12 / Коломинов Вячеслав Валентинович. Краснодар, 2017. 211 с.

306. Колычева А.Н. Фиксация доказательственной информации, хранящейся на ресурсах сети Интернет: автореф. канд. юрид. наук: 12.00.12 / Колычева Алла Николаевна. Москва, 2019. 25 с.

307. Колычева А.Н. Фиксация доказательственной информации, хранящейся на ресурсах сети Интернет: дис. ... канд. юрид. наук: 12.00.12 / Колычева Алла Николаевна. Москва, 2019. 199 с.

308. Костомаров К.М. Первоначальный этап расследования преступлений, связанных с незаконным доступом к компьютерной информации банков: дис. ... канд. юрид. наук: 12.00.09 / Костомаров Кирилл Валерьевич. Екатеринбург, 2012. 212 с.

309. Кот Е.А. Расследование преступлений, совершенных в сети Интернет, связанных с побуждением несовершеннолетних к суициду: дис. ... канд. юрид. наук: 12.00.12 / Кот Екатерина Александровна. Калининград, 2022. 326 с.

310. Кутузов А.В. Методологические основы раскрытия и расследования преступлений экстремистской направленности с использованием информационно-телекоммуникационной сети Интернет: дис. ... канд. юрид. наук: 12.00.12 / Кутузов Алексей Владимирович. Ростов-на-Дону, 2022. 237 с.

311. Летёлкин Н.В. Уголовно-правовое противодействие преступлениям, совершаемым с использованием информационно-телекоммуникационных сетей (включая сеть «Интернет»): дис. ... канд. юрид. наук: 12.00.08 / Летёлкин Николай Владимирович. Нижний Новгород, 2018. 218 с.

312. Льянов М.М. Криминалистическое значение электронно-цифровых следов преступлений экстремистской и террористической направленности в сети «Интернет»: дис. ... канд. юрид. наук: 5.1.4. / Льянов Муса Микаилович. Екатеринбург, 2025. 248 с.

313. Мазуров И.Е. Методика расследования хищений, совершенных с использованием Интернет-технологий: дис. ... канд. юрид. наук: 12.00.12 / Мазуров Игорь Евгеньевич. Ростов: 2017. 188 с.

314. Мочалкина И.С. Цифровые права и цифровая валюта как предмет преступлений в сфере экономики: дис. ... канд. юрид. наук: 5.1.4. / Мочалкина Ирина Сергеевна. Москова, 2022. 240 с.

315. Простосердов М.А. Экономические преступления, совершаемые в киберпространстве, и меры противодействия им: дис. ... канд. юрид. наук: 12.00.08 / Михаил Александрович Простосердов. Москва, 2016. 232 с.

316. Решняк О.А. Использование компьютерных технологий при расследовании преступлений в сфере незаконного оборота опасных психоактивных

веществ: дис. ... канд. юрид. наук: 12.00.12 / Решняк Ольга Александровна. Волгоград, 2020. 220 с.

317. Родина Е.А. Противодействие криминальной виктимизации пользователей сети «Интернет» в киберпространстве: дис. ... канд. юрид. наук: 5.1.4. / Родина Екатерина Анатольевна. Саратов, 2022. 217 с.

318. Сафонов О.М. Уголовно-правовая оценка использования компьютерных технологий при совершении преступлений: состояние законодательства и правоприменительной практики, перспективы совершенствования: дис. ... канд. юрид. наук: 12.00.08 / Сафонов Олег Михайлович. Москва, 2015. 222 с.

319. Себякин А.Г. Тактика использования знаний в области компьютерной техники в целях получения криминалистически значимой информации: дис. ... канд. юрид. наук: 12.00.12 / Себякин Алексей Геннадьевич Москва, 2021. 271 с.

320. Степанов-Егиянц В.Г. Методологическое и законодательное обеспечение безопасности компьютерной информации в российской федерации (уголовно-правовой аспект): дис. ... док. юрид. наук: 12.00.08 / Степанов-Егиянц Владимир Георгиевич. Москва, 2016. 389 с.

321. Столбова Н.А. Методика расследования незаконного оборота огнестрельного оружия с использованием информационно-телекоммуникационных сетей, в том числе сети «Интернет»: дис. ... канд. юрид. наук: 5.1.4. / Столбова Наталья Алексеевна. Иркутск, 2024. 243 с.

322. Трикоз Е.Н. Генезис и эволюция уголовно-правовой кодистики в традиции общего права: дис. ... док. юрид. наук / Трикоз Елена Николаевна. Москва, 2025. 503 с.

323. Туркулец В.А. Защита несовершеннолетних от преступных посягательств, совершаемых с использованием сети Интернет: дис. ... канд. юрид. наук: 5.1.4. / Туркулец Валентина Алексеевна. Москва, 2024. 249 с.

324. Турунова М.Н. Противодействие влиянию сети «Интернет» на преступное поведение несовершеннолетних: дис. ... канд. юрид. наук: 5.1.4. / Турунова Меруерт Нурлановна. Санкт-Петербург, 2023. 242 с.

325. Фролов М.Д. Уголовно-правовое и криминологическое противодействие мошенничеству в сфере компьютерной информации: дис. ... канд. юрид. наук: 12.00.08 / Фролов Михаил Дмитриевич. Москва, 2019. 211 с.

326. Харина Е.А. Особенности методики расследования мошенничества в сфере компьютерной информации: дис. ... канд. юрид. наук: 5.1.4. / Харина Елена Алексеевна. Краснодар, 2024. 248 с.

327. Шевченко Е.С. Тактика производства следственных действий при расследовании киберпреступлений: дис. ... канд. юрид. наук: 12.00.12 / Шевченко Елизавета Сергеевна. Москва, 2016. 249 с.

328. Шипулин Г.Ф. Предупреждение преступлений, совершаемых с использованием компьютерных сетей: дис. ... канд. юрид. наук: 5.1.4. / Шипулин Георгий Фаризович. Москва, 2024. 201 с.

329. Щурова А.С. Незаконный оборот наркотических средств и их аналогов с использованием компьютерных технологий (сети Интернет): уголовно-правовое и криминологическое исследование: дис. ... канд. юрид. наук: 12.00.08 / Щурова Анна Сергеевна. Санкт-Петербург, 2017. 256 с.

330. Чекунов И.Г. Криминологическое и уголовно-правовое обеспечение предупреждения киберпреступности: дис. ... канд. юрид. наук: 12.00.08 / Чекунов Игорь Геннадьевич. Москва, 2013. 223 с.

331. Челноков В.В. Компьютерная информация как предмет преступления в отечественном уголовном праве: дис. ... канд. юрид. наук: 12.00.08 / Челноков Владислав Валерьевич. Екатеринбург, 2013. 226 с.

332. Ягудин А.Н. Уголовная ответственность за нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей: дис. ... канд. юрид. нау : 12.00.08 / Ягудин Адель Наилевич. Москва, 2013. 201 с.

333. Alabdulatif A. Cybercrime and analysis of laws in Kingdome of Saudi Arabia: Science in Information System Security: a thesis for the Master’s Degree / Afnan Alabdulatif; University of Houston. Houston, 2018. 71 p. the Faculty of the Department of Information and Logistics Technology.

334. Imranuddin M. A Study of Cyber Laws in the United Arab Emirates: a thesis for the Master’s Degree / Mohammed Imranuddin, Rochester Institute of Technology (Dubai Campus). New-York, 2017. 112 p.

Отечественные научные статьи

335. Антонов О. Ю. Анализ цифровой информации как одна из задач криминалистического исследования компьютерных средств и систем / О.Ю. Антонов // Вестник криминалистики. — 2020. — № 2(74). — С. 17-23.

336. Баканов К.С., Васюков В.Ф. К вопросу о правовом регулировании эксплуатации беспилотных транспортных средств в отдельных странах Азии / К.С. Баканов, В.Ф. Васюков // Проблемы правоохранительной деятельности. — 2024. — № 3. — С. 58–63.

337. Барака А. Цифровой терроризм: как современные технологии способствуют росту экстремизма и финансированию терроризма / А. Барака // Финансовая безопасность. — 2025. — № 4. — С. 67–69.

338. Бастрыкин А. И. Выявление и расследование преступлений, совершенных с использованием информационно-коммуникационных технологий / А. И. Бастрыкин // Вестник Российской правовой академии. 2022. — № 4. — С. 88-94.

339. Бастрыкин А. И. Цифровые технологии современной криминалистики / А. И. Бастрыкин // Вестник Академии Следственного комитета Российской Федерации. — 2021. — № 2 (28). — С. 11-17.

340. Беккин Р. И. Исламское или мусульманское право? (К вопросу о правовых аспектах исламских финансов) / Р. И. Беккин // Проблемы современной экономики. — 2013. — № 4(48). — С. 429-430.

341. Беккин Р. И. Особенности шариатского надзора в исламских финансовых институтах: Современный опыт мусульманских и немусульманских стран / Р. И. Беккин // Вестник Санкт-Петербургского университета. — Экономика. — 2014. — № 3. — С. 148-164.

342. Бессонов А. А. Искусственный интеллект в преступлении: орудие или субъект? / А. А. Бессонов // Расследование преступлений: проблемы и пути их решения. — 2022. — № 3(37). — С. 28-32.

343. Бессонов А. А. О некоторых направлениях совершенствования криминалистического обеспечения расследования киберпреступлений / А. А. Бессонов // Расследование преступлений: проблемы и пути их решения. — 2024. — № 2(44). — С. 31-37.

344. Васюков В.Ф., Булыжкин А.В. Изъятие электронных носителей информации при расследовании преступлений: нерешенные проблемы правового регулирования и правоприменения // Российский следователь. 2016. — № 6. — С. 3-7.

345. Васюков В.Ф., Старжинская А.Н. К вопросу об организационных и процессуальных особенностях получения электронных данных при расследовании преступлений (опыт Китайской Народной Республики) / В.Ф. Васюков, А.Н. Стражинская // Вестник Московского университета МВД России. — 2024. — № 6. — С. 20-25.

346. Васюков В.Ф., Стражинская А.Н. Об оперативно-розыскных и следственных мерах противодействия легализации преступных доходов с использованием криптовалют / В.Ф. Васюков, А.Н. Стражинская // Российское право: образование, практика, наука. — 2024. — № 4. — С. 68-78.

347. Вехов В.Б., Смагоринский Б.П., Ковалев С.А. Электронные следы в системе криминалистики / В.Б. Вехов, Б.П. Смагоринский, С.А. Ковалев // Судебная экспертиза. — №2. — С. 10–19.

348. Волеводз А.Г. Международная правоохранительная деятельность и международные правоохранительные организации: определение понятий / А.Г. Волеводз // Евразийский юридический журнал. — 2010. — № 11(30). — С. 128–134.

349. Волеводз А.Г. Международное сотрудничество в сфере уголовного судопроизводства – уроки истории и некоторые проблемы реформирования / А.Г. Волеводз // Библиотека криминалиста. Научный журнал. — 2014. — № 6 (17). — С. 281–288.

350. Волеводз А.Г. О необходимости имплементации в УПК РФ международно-правовых норм о новых направлениях международного сотрудничества в сфере уголовного судопроизводства / А.Г. Волеводз // Библиотека криминалиста. Научный журнал. — 2014. — № 4(14). — С. 311–328.

351. Волеводз А. Г., Решетников Ю. Г. Электронные доказательства в уголовном процессе Китайской Народной Республики / А. Г. Волеводз, Ю. Г. Решетников // Вестник экономической безопасности. — 2024. — № 5. — С. 20-27.

352. Волеводз А.Г., Цыплакова А.Д. Международное полицейское сотрудничество: современная институциональная структура и тенденции развития / А.Г. Волеводз, А.Д. Цыплакова // Международное уголовное право и международная юстиция. — 2023. — № 3. — С. 2-6.

353. Волеводз А.Г., Цыплакова А.Д. Уголовная ответственность юридических лиц в Королевстве Саудовская Аравия / А.Г. Волеводз, А.Д. Цыплакова // Российский следователь. — 2023. — № 11. — С. 57-61.

354. Волеводз А.Г., Цыплакова А.Д. Уголовная ответственность юридических лиц в Объединенных Арабских Эмиратах / А.Г. Волеводз, А.Д. Цыплакова // Российский следователь. — 2023. — № 12. — С. 58-62.

355. Волеводз А.Г., Цыплакова А.Д. Уголовная ответственность юридических лиц в Объединённых Арабских Эмиратах и Королевстве Саудовская Аравия: сравнение материальных и процессуальных аспектов / А.Г. Волеводз, А.Д. Цыплакова // Российский следователь. — 2024. — № 3. — С. 51–56.

356. Волеводз А.Г., Цыплакова А.Д. Цифровые доказательства в уголовном процессе государств-членов Совета сотрудничества арабских государств Персидского залива: правовой статус и процедуры / А.Г. Волеводз, А.Д. Цыплакова // Вестник экономической безопасности. — 2024. — № 2. — С. 21–29.

357. Дорошков В. В. К вопросу об уголовном проступке / В. В. Дорошков // Мировой судья. — 2016. — № 12. — С. 31-39.

358. Захарцев С.И., Кийко А.Ю., Семенова И.В. Цифровая информация как квалифицирующий признак формирования частной методики расследования преступлений / С.И. Захарцев, А.Ю. Кийко, И.В. Семенова // Юридическая наука: история и современность. — 2022. — № 11. — С. 126-134.

359. Зиновьева Е., Игнатов А. БРИКС в глобальном режиме ИКТ-безопасности / Е. Зиновьева Е., А. Игнатов // Международные процессы. — 2023. — № 21 (4). — С. 104-132.

360. Дамирчиев Э.И., Васюков В.Ф. Некоторые вопросы противодействия дистанционным мошенничествам в Китае // Э.И.Дамирчиев, В.Ф. Васюков / Научный вестник Орловского юридического института МВД России имени В.В. Лукьянова. — 2024. — № 2(99). — С. 161-166.

361. Долгиева М. М. Цифровой объект преступления / М. М. Долгиева // Вестник Томского государственного университета. — 2022. — № 483. — С. 253-260.

362. Долгиева М. М. Цифровой ущерб от преступления: практические вопросы / М. М. Долгиева // Вестник Томского государственного университета. — 2023. № 487. — С. 206-211.

363. Иванов И. И., Кондрат И.Н. Особенности предупреждения преступлений, совершенных с использованием современных информационно-телекоммуникационных технологий / И. И. Иванов, И. Н. Кондрат // Мировой судья. — 2024. — № 12. — С. 2-9.

364. Клевцов К. К. Международное сотрудничество в борьбес киберпреступностью в контексте противодействия новым вызовам и угрозам / К. К. Клевцов // Вестник Санкт-Петербургского университета. Право. — 2022. — Т. 13. № 3. — С. 678-695.

365. Клевцов К. К. Особенности взаимодействия правоохранительных органов с зарубежными поставщиками услуг виртуальных валют (на примере LocalBitcoins) / Клевцов К. К. // Вестник Московского университета МВД России. — 2023. — № 1. — С. 139-145.

366. Лун Ч. Состав преступления в уголовно-правовой доктрине Китая / Ч. Лун // Lex Russica. — 2016. — № 9. — С. 129-135.

367. Подшибякин А.С. О технологиях и искусстве в криминалистике // Юридическая техника. 2015. № 9. — С. 569-571.

368. Поляков И.С. Особенности элементов механизма образования электронных следов в сети Интернет / И.С. Поляков // Сибирские уголовно-процессуальные и криминалистические чтения. — 2025. — № 2.— С. 70–81.

369. Поляков И. С. Понятие, классификация электронных следов и их криминалистическое значение / И.С. Поляков // Вестник Академии Следственного комитета Российской Федерации. — 2024. — № 4(42). — С. 169-176.

370. Россинская Е.Р., Семикаленова А.И. Основы учения о криминалистическом исследовании компьютерных средств и систем как часть теории информационно-компьютерного обеспечения криминалистической деятельности // Вестник Санкт-Петербургского университета. Право. — 2020. — № 11(3). — С. 745-759.

371. Рыжкова Е. А. Становление и развитие права стран Африканского континента: общие вопросы / Е. А. Рыжкова // Право между Востоком и Западом. — 2024. — № 1.— С. 30-38.

372. Рыжкова Е. А., Мельник С.С. Международное сотрудничество в сфере уголовного судопроизводства: опыт Мальты / Е. А. Рыжкова, С. С. Мельник // Электронное приложение к Российскому юридическому журналу. — 2023. — № 1. — С. 21-26.

373. Сидоренко Э. Л. Defi-преступность: состояние, тенденции и криминологические модели / Э.Л. Сидоренко // Russian Journal of Economics and Law. — 2023. — Т. 17. — № 2. — С. 327-341.

374. Синякин И. И. Перспективы международно-правового сотрудничества по борьбе с терроризмом / И.И. Синякин // Московский журнал международного права. — 2017. — № 1(105). — С. 78-87.

375. Сукманов А. О. Сущность, понятие и виды электронно-цифровых следов, используемых в раскрытии и расследовании преступлений / А.О. Сукманов // Вестник Калининградского юридического института МВД России. — 2010. — № 4 (22). — С. 104-107.

376. Сюкияйнен Л.Р. Особенности современного исламского права / Л.Р. Сюкияйнен // Право между Востоком и Западом. — 2025. — № 2. — С. 28–41.

377. Шестак В.А., Волеводз А.Г. Современные потребности правового обеспечения искусственного интеллекта: взгляд из России / В.А. Шестак, А.Г. Волеводз // Всероссийский криминологический журнал. — 2019. — № 13 (2). — С. 197-206.

378. Шестак В.А., Цыплакова А.Д. Понятие и сущность киберпреступлений в государствах-членах ССАГПЗ / В.А. Шестак, А.Д. Цыплакова // Мировой судья. — 2023. — № 4. — С. 2–7.

379. Шестак В.А., Цыплакова А.Д. Проблемы определения и классификации экономических преступлений в ОАЭ / В.А. Шестак, А.Д. Цыплакова // Уголовное право: стратегия развития в XXI веке. — 2023. — № 2. — С. 273-281.

380. Шестак В.А., Цыплакова А.Д. Проблемы регулирования уголовной юрисдикции в Королевстве Саудовская Аравия / В. А. Шестак, А.Д. Цыплакова // Мировой судья. — 2023. — № 2. — С. 2–6.

381. Шестак В.А., Цыплакова А.Д. Проблемы регулирования уголовной юрисдикции в Объединённых Арабских Эмиратах / В.А. Шестак, А.Д. Цыплакова // Российский следователь. — 2023. — № 7. — С. 65–68.

382. Шестак В.А., Цыплакова А.Д. Проблемы совершенствования прогнозирования преступности / В.А. Шестак, А.Д. Цыплакова // Расследование преступлений: проблемы и пути их решения. — 2023. — № 3 (41). — С. 78–84.

383. Шестак В.А., Цыплакова А.Д. Противодействие отмыванию денежных средств, полученных преступным путем: опыт Объединенных Арабских Эмиратов/ В.А. Шестак, А.Д. Цыплакова // Вестник Университета прокуратуры Российской Федерации. — 2023. — № 4 (96). — С. 117–122.

384. Цыплакова А.Д. Борьба с киберпреступностью в странах Глобального Юга: сравнительно-правовое исследование // Пролог: журнал о праве. — 2025. — № 1. — С. 99–110.

385. Цыплакова А.Д. Должностные лица и органы, обеспечивающие реализацию полноты судебной власти, в арабских государствах: понятие и полномочия / А.Д. Цыплакова // Вестник Дальневосточного юридического института МВД России имени И.Ф. Шилова. 2025. — № 2 (71). — С. 142-151.

386. Цыплакова А.Д. Концептуализация понятия «(страны) Глобального Юга»: диффузия повседневной речи, научной терминологии и специализированных дискурсов в призме лингвокультурологии / А.Д. Цыплакова // Концепт: философия, религия, культура. — 2025. — № 9 (2). — С. 116-134.

387. Цыплакова А.Д. Международное сотрудничество в борьбе с киберпреступлениями: некоторые правовые проблемы в свете принятия Конвенции ООН против киберпреступности / А.Д. Цыплакова // Российский следователь. — 2025. — № 10. — С. 62-66;

388. Цыплакова А.Д. Противодействие киберпреступлениям в странах Глобального Юга: современное состояние, проблемы и перспективы / А.Д. Цыплакова // Право и управление. XXI век. — 2025. — № 3. — С. 62–75.

389. Цыплакова А.Д. Некоторые юрислингвистические особенности источников уголовного права и уголовного процесса арабских государств / А.Д. Цыплакова // Право между Востоком и Западом. — 2025. — № 1. — С. 28–38.

390. Яковенко А.В. Картина нарождающегося мира: Глобальный Юг / А.В. Яковенко // Проблемы национальной стратегии. — 2024. — № 1 (82). — С. 42–57.

391. Ivanov D., Grinenko A., Fadeev P., Ermakov S., Antimonova S. Comparative Legal Analysis of the Use of Electronic Format of Criminal Cases and the Procedure under the Code of Criminal Procedure of the Russian Federation / D. Ivanov, A. Grinenko, P. Fadeev, S. Ermakov, S. Antimonova // Jurnal Cita Hukum. 2024. — Vol. 12. — No. 2. — P. 309-320.

392. Shestak V.A., Tsyplakova A.D. Classification of cybercrimes in GCC countries / V.A. Shestak, A.D. Tsyplakova // Law, State and Telecommunications Review. 2024. № 16-1. P. 65–78.

393. Shestak V.A., Tsyplakova A. D. Countering Cyberattacks on the Energy Sector in the Russian Federation and the USA / V.A. Shestak, A. D. Tsyplakova // BRICS Law Journal. — 2023. — Vol. 10. — No. 4. — P. 35–52.

394. Shestak V.A., Tsyplakova A.D. Criminological features of the cybersecurity threats / V.A. Shestak, A.D. Tsyplakova // Law, State and Telecommunications Review. — 2023. — No. 15-2. — P. 187–203.

395. Shestak V.A., Tsyplakova A.D. Judge requirements and ethical issues in the Cooperation Council for the Arab States of the Gulf / V.A. Shestak, A. D. Tsyplakova // Vestnik of Saint Petersburg University. Law. — 2024. — Vol. 15. — No. 2. — P. 493-507.

396. Trikoz E. N. Ethical and Legal Landscape of Blockchain in Genetic Research / E. N. Trikoz, N. O. Sidorova, E. E. Gulyaeva // Lex Genetica. — 2025. Vol. 4. — No. 1. — P. 54-66.

397. Tsyplakova A.D. Comprehensive approach to cybercrime prevention in Arab countries / A.D. Tsyplakova // Law, State and Telecommunications Review. — 2025. — № 17-1. — P. 23–41.

Зарубежные научные статьи

398. Abu-taieh E., Alotaibi Sh., Aldehim Gh., Alfaries A. A. Cyber Security Crime and Punishment: Comparative Study of the Laws of Jordan, Kuwait, Qatar, Oman, and Saudi Arabia / E. Abu-taieh, Sh. Alotaibi, Gh. Aldehim, A. A. Alfaries // International Journal of Cyber Warfare and Terrorism. — 2018. — № 8 (3). — P. 46–59.

399. Aissani R. Anti-Cyber and information technology crimes laws and legislation in the GCC countries: A comparative analysis study of the laws of the UAE, Saudi Arabia and Kuwait / R. Aissani // Journal of Legal, Ethical and Regulatory Issues. — 2022. — № 25(1). — P. 1–14.

400. Aissani R. The Ethics and Legislation of the New Media Use in the United Arab Emirates Analytical Study of the Law - Combating IT Crimes / R. Aissani // AAU Journal of Business and Law. — 2020. — № 2 (1). — P. 72–98.

401. Ajala I., Shanaz F., El Barachi M., Oroumchian F., Sujith M., Rand Y., Lutfi S. Combining artificial intelligence and expert content analysis to explore radical views on twitter: case study on far-right discourse / I.Ajala, F. Shanaz, M. El Barachi, F. Oroumchian, M. Sujith, Y. Rand, S. Lutfi // Journal of Cleaner Production. — 2022. — № 362. — 132263.

402. Ajijola A.-H., Allen Nate D.F. African Lessons in Cyber Strategy / A.-H. Ajijola, D.F. Allen Nate // Africa Center for strategic studies. — 08.03.2022. — URL: https://africacenter.org/spotlight/african-lessons-in-cyber-strategy/ (accessed 04.05.2025).

403. Al-Saud N. B. A. A Saudi Outlook for Cybersecurity Strategies Extrapolated from Western Experience / N. B. A. Al-Saud // Joint Force Quarterly. — 2012. — № 64. — P. 75–81.

404. Al-Shibli K. Agency (Wakala) and its applications in Islamic banking / K. Al-Shibli // Journal of Islamic Economics, Banking and Finance. — 2020. — № 16(3). — P. 1-15.

405. Algabri Z.A.N., Abdul Shukor S., Mohammed Hasan B.M. Evidence and investigation of Internet crimes in UAE / Z.A.N. Algabri, Abdul S. Shukor, B.M Mohammed Hasan // Al-Hikmah: International Journal of Islamic Studies and Human Sciences. — 2022. — № 5 (2). — P. 228–251.

406. Alqurashi R. K., AlZain M. A., Soh B., Masud M., Al-Amri J. Cyber Attacks and Impacts: A Case Study in Saudi Arabia / R. K. Alqurashi, M. A. AlZain, B. Soh, M. Masud, J. Al-Amri // International Journal of Advanced Trends in Computer Science and Engineering. — 2020. — № 9 (1). — P. 217-234.

407. Ardiyanti H. Cybersecurity dan Tantangan Pengembangannya di Indonesia / H. Ardiyanti // Jurnal Politica. — 2014. — № 5 (1). — P. 1–16.

408. Bara Pratama Mahaputra, Chairul Muriman, Surya Nita. Use Of Digital Forensic Technology To Reveal The Identity Of Social Engineering Crimes / Bara Pratama Mahaputra, Chairul Muriman, Surya Nita // Riwayat Educational Journal of History and Humanities. — 2024. — № 7 (3). — P. 1000–1008.

409. Barlian A.A.E., Latipulhayat A., Rusmiati E., Wulandari W., Sukma A.N.A. Electronic Criminal Justice in Indonesia: Challenges and the Future Measures / A.A.E. Barlian, A. Latipulhayat, E. Rusmiati, W. Wulandari, A.N.A. Sukma // Jambura Law Review. — 2025. — № 1(7). — P. 243–274.

410. Bruce M., Lusthaus J., Kashyap R., Phair N., Varese F. Mapping the global geography of cybercrime with the World Cybercrime Index / M. Bruce, J.Lusthaus, R. Kashyap, N. Phair, F. Varese // PLoS ONE. — 2024. — №. 19(4). — e0297312.

411. Chaitali J. C.S., Rathor S.P. A Legal Framework for Determining The Criminal Liability And Punishment For Artificial Intelligence / J.C.S. Chaitali, S.P. Rathor // Tuijin Jishu / Journal of Propulsion Technology. — 2024. — № 45 (1). — P. 807–820.

412. Creemers R. The Chinese Conception of Cybersecurity: A Conceptual, Institutional and Regulatory Genealogy / R. Creemers // Journal of Contemporary China. — 2023. — № 33 (146). — P. 173–188.

413. Draganova R., Ross B., Wollbrink A., Pantev C. Cortical steady-state responses to central and peripheral auditory beats / R. Draganova, B. Ross, A. Wollbrink, C. Pantev // Cereb cortex. — 2007. — № 18(5). — P. 1193-1200.

414. El-Kady R.M. Handling E-evidence in Egyptian and Comparative Legislation: A Comparative Analytical Study / R.M. El-Kady // Arab Journal of Forensic Sciences and Forensic Medicine. — 2023. — № 5 (2). — P. 191–222.

415. El-Kady R. The Authenticity of Digital Evidence Before Criminal Courts / R. El-Kady // ResearchGate. — 01.2024. — URL: https://www.researchgate.net/publication/377527331_The_Authenticity_of_Digital_Evidence_Before_Criminal_Courts (accessed 01.05.2025) (in Arabic).

416. Estiyovionita K., Sitamala A. ASEAN's role in cybersecurity maintenance and security strategy through an international security approach / K. Estiyovionita, A. Sitamala // LaJiL. — 2022. — № 4 (2). — P. 79-86.

417. Fawzi M.M., Mansouri F.A. Awareness on Digital Drugs Abuse and its Applied Prevention Among Healthcare Practitioners in KSA / M.M. Fawzi, F.A. Mansouri // AJFSFM. — 2017. — № 1 (6). — P. 625–633.

418. Flore J. Ingestible sensors, data, and pharmaceuticals: subjectivity in the era of digital mental health / J. Flore // New Media Soc. — 2021. — № 23. — P. 2034–2051.

419. Ghamami S.M.M., Alipoor M. A comparative study of exposure to cryptocurrencies in the Iranian and American legal systems / S.M.M. Ghamami, M. Alipoor // Encyclopedia of Economic Law Journal. — 2022. — № 29(21). — P. 150-184 (in Persian).

420. Ghuman A. Elements of Crime / A. Ghuman // International Journal of Law Management & Humanities. — 2018. — № 1 (4). — P. 1–18.

421. Hadar A., Hadas I., Lazarovits A., Alyagon U., Eliraz D., Zangen A. Answering the missed call: Initial exploration of cognitive and electrophysiological

changes associated with smartphone use and abuse / A. Hadar, I. Hadas, A. Lazarovits, U. Alyagon, D. Eliraz, A. Zangen // PLOS ONE. — 2017. — № 12(7). — Article e0180094.

422. Kaburuan E.D., Damayanti A. The Effectiveness of Indonesian National Police Strategy in Cybercrime eradication through ASEAN Ministerial Meeting on Transnational Crime (AMMTC) / E.D. Kaburuan, A. Damayanti // International Journal of Social Science and Human Research. — 2022. — № 5 (8). — P. 3649-3661.

423. Khaled Eid. The Role of the Law in Protecting Individuals from Electronic Blackmail / K. Eid // Journal of Public Policy and Administration. — 2024. — № 8 (3). — P. 103–108.

424. Lasledj N., Bouzoualeg Kh. Electronic elections in Algeria: between reality and expectations comparative study with the Omani experience / N. Lasledj, Kh. Bouzoualeg // Russian Law Journal. — 2025. — № 13 (1). — P. 447–456.

425. Maarouf K. Procedural Problems Facing a Criminal Investigator in Cybercrimes / K. Maarouf // Arab Journal of Forensic Sciences and Forensic Medicine. — 2022. — № 4 (2). — P. 158–166.

426. Maleh Ya., Maleh Yo. The Moroccan View on Cybersecurity / Ya. Maleh, Yo. Maleh // Cybersecurity in Morocco / ed. by Ya. Maleh, Yo. Maleh. — Springer Cham, 2022. — P. 41–50.

427. Manthovani R. Implementation of Criminal Law in Indonesia / R. Manthovani // YURISDIKSI: Jurnal Wacana Hukum Dan Sains. — 2021. — № 16 (4). — P. 266–274.

428. Masadeh A. M. S. Combating Cyber Crimes — Legislative Approach — A comparative Study (Qatar, UAE, UK) // Законодательная база Государства Катар «al-Meezan»: сайт. — URL: https://www.almeezan.qa/ReferenceFiles.aspx?id=54&type=doc&language=en (дата обращения: 09.03.2025).

429. McConnell P.A., Froeliger B., Garland E.L., Ives J.C., Sforzo G.A. Auditory driving of the autonomic nervous system: Listening to theta-frequency binaural beats post-exercise increases parasympathetic activation and sympathetic withdrawal / P.A. McConnell, B. Froeliger, E.L. Garland, J.C. Ives, G.A. Sforzo // Front Psychol. — 2014. — № 5:1248.

430. Nashriana N.A.A., Isma Nurillah I. Persidangan Perkara Pidana Di Pengadilan Secara Elektronik Pada Masa Pandemi Covid-19 Ditinjau Dari Asas Peradilan Pidana / N.A.A. Nashriana, I. Isma Nurillah // Simbur Cahaya. — 2021. — № 28 (1).

431. Patil H.B., Chowbe A. An Examination Of Digital Evidence And Its Relevance For Indian Forensic / H.B. Patil, A. Chowbe // Educational Administration: Theory and Practice. — 2024. — № 30(5). — P. 6445–6452.

432. Plowman R.S., Peters-Strickland T., Savage G.M. Digital medicines: clinical review on the safety of tablets with sensors / R.S. Plowman, T. Peters-Strickland, G.M. Savage // Expert Opin Drug Saf. — 2018. — №17. — P. 849–852.

433. Purnomo H. Criminal liability for the use of artificial intelligence in Indonesia / H. Purnomo // Jurnal Info Sains: Informatika dan Sains. — 2023. — № 13 (3). — P. 1109–1114.

434. Rizal M., Yani Y.M. Cybersecurity Policy and Its Implementation in Indonesia / M. Rizal, Y.M. Yani // Journal of ASEAN Studies. — 2016. — № 4 (1). — P. 61–78.

435. Sayyed H. Artificial intelligence and criminal liability in India: exploring legal implications and challenges / H. Sayyed // Cogent Social Sciences. — 2024. — № 10(1). — Article 2343195.

436. Saputro H.D., Fatoni S. Persidangan Perkara Pidana Secara Elektronik Dalam Sistem Peradilan Pidana Di Indonesia Di Masa Pandemi Covid-19 / H.D. Saputro, S. Fatoni // INICIO LEGIS. — 2022. — № 3 (2). — P. 142–161.

437. Seawright J., Gerring J. Case Selection Techniques in Case Study Research // Political Research Quarterly. — 2008. — № 61. — P. 294-308.

438. Setiadi F., Sucahyo Y.G., Hasibuan Z.A. An Overview of the Development Indonesia National Cyber Security / F. Setiadi, Y.G. Sucahyo, Z.A. Hasibuan // International Journal of Technology & Computer Science. — 2012. — №6. — P. 106–114.

439. Shires J., Hassib B. Cybersecurity in the GCC: From Economic Development to Geopolitical Controversy / J. Shires, B. Hassib // Middle East Policy. — 2022. — № 29 (1). — P. 90–103.

440. Siham L., Safia S. Legal criminal mechanisms for combating cybercrime in Algerian legislation / L. Siham, S. Safia // Russian Law Journal. — 2025. — № 1. — P. 52–61.

441. Vladeck D.C. Machines without principals: Liability rules and artificial intelligence / D.C. Vladeck // Washington Law Review. — 2014. — № 89(1). — P. 117–150.

442. Vicente A., Lavazza A. Artificial intelligence, legal personhood and the non-reductive materialist perspective / A. Vicente, A. Lavazza // International Journal of Law and Information Technology. — 2020. — № 28(2). — P. 146–162.

443. Yaghla M., Kenaza S. Digitization of litigation procedures in algeria: between consolidating the modernization of justice and violating the fundamental principles of litigation / M. Yaghla, S. Kenaza // Russian Law Journal. — 2025. — Vol. 1. — P. 1141–1156.

444. Yilma K.M. Some Remarks on Ethiopia’s New Cybercrime Legislation / K.M. Yilma // Mizan Law Review. — 2016. — № 10 (2). — P. 448–458.

445. Yilma K.M., Abraha H.H. The Internet and Regulatory Responses in Ethiopia: Telecoms, Cybercrimes, Privacy, E-commerce, and the New Media / K.M. Yilma, H.H. Abraha // Mizan Law Review. — 2015. — № 9 (1). — P. 108–153.

446. Won C., Kwon C., Park K., Seo J., Lee T. Electronic Drugs: Spatial and Temporal Medical Treatment of Human Diseases / C. Won, C. Kwon, K. Park, J. Seo, T. Lee // Advanced Materials. — 2021. — Article 2005930.

447. Zulaeha M. E-Courts in Indonesia: Exploring the Opportunities and Challenges for Justice and Advancement to Judicial Efficiency / M. Zulaeha // International Journal of Criminal Justice Sciences. — 2023. — № 18 (2). — P. 183–194.

448. Хамудату Аль-Махмуд Али. Доказательства киберпреступлений, умысел и оценка в рамках теории доказательств по уголовным делам / Аль-Махмуд Али Хамудату // Журнал безопасности и права. — 2003. — № 1. — С. 9–95 (на араб. яз.)

449. الحوامدة، لورانس. حجيَّة الأدلة الرقميَّة في الإثبات الجنائيّ: دراسة تحليليَّة مُقارنة // مجلة البحوث الفقهيَّة والقانونيَّة. ٢٠٢١. ٣٦. ٨٨٣-٩٣٦ ص. [Аль-Хавамдех Л. Допустимость цифровых доказательств в уголовном судопроизводстве: Сравнительное аналитическое исследование / Л. Аль-Хавамдех // Журнал юриспруденции и правовых исследований. — 2021. — № 36. — С. 883–936].

450. لد الصديق ميلود. الوسائط الرقمية الحديثة من شبكات التواصل الاجتماعي // مجلة أكاديميا. ٢٠١٦. ٤. ١٩٣-٢١١ [Сиддик Милуд. Современные цифровые медиа из социальных сетей / Милуд Сиддик // Академический журнал. — 2016. — № 4. — С. 193–211].

451. الهمداني ميسون خلف حمد الحمداني. مشروعية الدليل الإلكتروني كدليل في القضايا الجنائية // مجلة كلية الحقوق لجامعة النهرين. ٢٠١٦. ١٨. ٢. ١٩٥-٢٥٤ ص. [Аль-Хамдани Мэйсун Халаф Хамад. Законность электронных доказательств в качестве доказательств по уголовному делу / М.Х.Х. Аль-Хамдани // Журнал колледжа права Университета Аль-Нахрэйн. — 2016. — № 18 (2). — С. 195–254].

452. نفيد ي. المكافحة التشريعية لبعض صور الجرائم المعلوماتية وأصناف المجرم المعلوماتي // المجلة العربية للدراسات الأمنية. ٢٠٢٢. ٣٨ (٢). ١٣٧-١٤٥ [Навид Ю. Законодательный контроль над некоторыми формами киберпреступности и типами киберпреступников / Ю. Навид // Арабский журнал исследований в области безопасности. — 2022. — № 38(2). — С. 137–145].

453. العنزي م. الجانب الموضوعي للاحتيال من خلال المواقع الإلكترونية في النظام السعودي مقارنًا بالقانونين المصري والكويتي // المجلة العربية للدراسات الأمنية. ٢٠٢٢. ٣٨ (١). ٠٤-١٧ ص. [Аль-Энези М. Содержательный аспект мошенничества с использованием веб-сайтов в саудовской системе по сравнению с египетским и кувейтским законодательством / М. Аль-Энези // Арабский журнал исследований в области безопасности. — 2022. — № 38 (1). — С. 04–17].

454. الهياس , خولة موسى , استغلال وسائل تقنية المعلومات في ارتكاب جرائم المخدرات وخاصة الرقمية : في ضوء قانون مكافحة جرائم تقنية المعلومات الاماراتي // مجلة العلوم الاقتصادية والإدارية والقانونية. ٢٠١٨. ٩. ٢. ١٦٨-١٨١ ص [Аль-Хайас Хавла Мусса. Использование информационных технологий при совершении наркопреступлений, особенно цифровых: В свете закона ОАЭ о киберпреступности / Х.М. Аль-Хайас // Журнал экономических, административных и юридических наук. — 2018. — № 9(2). — С. 168–181].

455. آل خطاب، خميس عبد ربه منشور. التكييف القانوني للمخدرات الرقمية على قيام المسؤولية الجزائية في التشريع الأردني // مجلة جامعة الحسين بن طلال للبحوث. ٢٠٢١. ٧ (٢). ١٧٠-٢٠٣ ص [Аль-Хатаб Хамис Абд Раббу Маншур. Правовая характеристика цифровых наркотиков с точки зрения установления уголовной ответственности в законодательстве Иордании / Х.А.Р.М. Аль-Хатаб // Научно-исследовательский журнал Университета Аль-Хусейн бин Талал. — 2021. — № 7 (2). — С. 170–203].

456. ليلى ميسوم. المخدرات الرقمية: ظهور إدمان جديد عبر شبكة الإنترنت // مجلة جيل العلوم الإنسانية والاجتماعية. ٢٠١٢. ٢١. ١٦٣-١٧٤ ص [Мессум Лейла. Цифровые наркотики: Возникновение новой онлайн-зависимости / Л. Мессум // Журнал «Поколение гуманитарных и социальных наук». — 2012. — № 21. — С. 163–174].

457. عبد الله ا.، سيد م. الأحكامُ الموضوعيَّة لجريمتي الإخفاء والعبث بالدليل الرقميِّ في التشريعين الإماراتيّ والمصريّ (دراسة مُقارنة) // مجلة جامعة الشارقة للعلوم القانونية. ٢٠٢٤. ٢١. ٤. ١٧٦-١٩٨ ص. [Абдулла И., Сайид М. Основные положения о преступлениях сокрытия и фальсификации цифровых доказательств в законодательстве ОАЭ и Египта (сравнительное исследование) / И. Абдулла, М. Сайид // Журнал университета Шарджи юридических наук. — 2024. — № 21 (4). — С. 176–198].

458. القاضي ر. الدليل الجنائي الرقمي في تقنية الميتافيرس // المجلة العربية للدراسات الأمنية. ٢٠٢٣. ٣٩. (٢). ١٨٩-٢٠٤ ص. [Аль-Кади Р. Цифровые судебные доказательства в технологии Metaverse / Р. Аль-Кади // Арабский журнал исследований в области безопасности. — 2023. — № 39(2). — С. 189–204].

459. حجية الدليل الالكتروني في الاثبات الجنائي وسمطة القاضي في تقديره. محمود صبحي محمد محمود ا زيد [Заид Махмуд Собхи Мухаммад Махмуд. Авторитетность электронных доказательств в уголовном деле и дискреционные полномочия судьи] / М.С.М.М. Заид // Журнал гуманитарных наук Бехна. — 2022. — № 1 (2). — С. 27–48.

460. البلوي غ. الأبعاد القانونيَّة لاستخدام الروبوتات في الأعمال الإرهابية في النظام السعودي // المجلة العربية للدراسات الأمنية.٢٠٢٤. ٤٠ (١). ٤-١٣ ص [Аль-Балави Г. Правовые аспекты использования роботов в террористических актах в системе Саудовской Аравии / Г. Аль-Балави // Арабский журнал исследований безопасности. — 2024. — № 40(1). — С. 4–13].

461. خالد علي نازل الشعار. التحقيق الجنائي في الجرائم الإلكترونية [Аш-Шаар Халид Али Назал. Уголовное расследование электронных преступлений] / Х.А.Н. Аш-Шаар // Журнал юридических и экономических исследований. — 2022. — № 12 (79). — С. 133–183.

462. قانصو علي. الحرب الإلكترونية // مجلة الدفاع الوطني البناني. ٢٠٢١. ١١٨. ٣-٣٥ ص [Кансо Али. Электронная война / А. Кансо // Журнал национальной обороны Ливана. — 2021. — № 118. — С. 3–35].

463. مبارك بن محمد الخالدي. الإثبات بالدليل الرقمي وتطبيقاته القضائية: دراسة فقهية مقارنة بنظام الإثبات السعودي. [Аль-Халиди Мубарак бин Мухаммад. Доказательство с помощью цифровых доказательств и его судебное применение: юриспруденческое исследование в сравнении с саудовской системой доказательств / Мубарак бин Мухаммад Аль-Халиди // Судебный журнал. — 2024. — С. 329-416].

464. هادی تبار, اسماعیل, یعقوبی گلوردی, محمد کاظم. ادله اثبات الکترونیکی در دادرسی‌های کیفری در نظام حقوقی ایران // فقه جزای تطبیقی. ۲۰۲۳. ۳ (۱). ۱۲۳-۱۱۳. [Табар Хади, Исмаил, Якуби Глорди Мохаммад Казем. Доказательства электронных доказательств в уголовном процессе в правовой системе Ирана / Х. Табар, И. Исмаил, М.К. Якуби Глорди // Сравнительное уголовное правоведение. — 2023. — № 3 (1). — С. 113–123].

465. خسروی زاد, افشار, سپهری, روح الله, بابایی, حمیده. مشروعیت تحصیل دلیل در جرایم فضای مجازی در حقوق جزایی ایران // فقه جزای تطبیقی. ۲۰۲۲. ۲ (۳). ۸۵-۷۵ [Хосравизад Афшар, Сепери Рухолла, Бабаи Хамида. Легитимность изучения доказательств преступлений в киберпространстве в уголовном праве Ирана / А. Хосравизад, Р. Сепери, Х. Бабаи // Сравнительное уголовное правоведение. — 2022. — № 2 (3). — С. 75–85].

466. محمد محمود الكمالي. أحكام التعاون القضائي الدولي في المسائل الجنائية في دولة الإمارات العربية المتحدة [Аль-Камали Мухаммад Махмуд. Положение о международном судебном сотрудничестве по уголовным делам в Объединенных Арабских Эмиратах] / Мухаммад Махмуд Аль-Камали // Журнал судебных исследований Министерства юстиции ОАЭ. — № 3. — URL: https://elaws.moj.gov.ae/Adel.aspx?val=UAE-FokehAA1 (дата обращения: 18.12.2024).

Материалы конференций

467. Бессонов А.А. Искусственный интеллект как орудие преступлений и средство их расследования / А.А. Бессонов // Государственная научно-техническая политика в сфере криминалистического обеспечения правоохранительной деятельности: сборник научных статей по материалам международной научно-практической конференции, Москва, 26 мая 2023 года / Академия управления МВД России. Том Часть 1. — Москва: Академия управления Министерства внутренних дел Российской Федерации, 2023. — С. 10-17.

468. Гриненко А. В. Современные проблемы межведомственного взаимодействия следственных органов / А.В. Гриненко // Особенности противодействия гибридным угрозам в отношении Российской Федерации: Материалы Луганского международного юридического форума, Луганск, 14 мая 2024 года. — Луганск: Луганская академия Следственного комитета Российской Федерации, 2024. — С. 51-55.

469. Скобелин С.Ю. Сложные вопросы расследования киберпреступлений / С.Ю. Скобелин // Советская и российская криминалистика: традиции и современные векторы: Материалы всероссийской научно-практической конференции, Москва, 29 февраля 2024 года. — Москва: Московская академия Следственного комитета им. А.Я. Сухарева, 2024. — С. 228-231.

470. Старжинская А.Н. Современный подход к расследованию в отношении активов, полученных в результате совершения преступлений / А.Н. Старжинская // Уголовный процесс и криминалистика:правовые основы, теория, практика, дидактика (к 75-летию со дня рождения профессора Б. Я. Гаврилова): сборник научных статей по материалам международной научно-практической

конференции, Академия управления МВД России, 03 ноября 2023 года. — Москва: Академия управления МВД России, 2023. — С. 391-396.

471. Хатов Э.Б. Киберполигон как платформа цифровых компетенций следователей криминалистов / Э.Б. Хатов // Советская и российская криминалистика: традиции и перспективы: Материалы всероссийской научно-практической конференции с международным участием, Москва, 02 февраля 2023 года. Москва: Московская академия Следственного комитета Российской Федерации, 2023. — С. 210-213.

472. Хишам Мухаммад Харид Растум. Информационные преступления: истоки технического уголовного расследования / Хишам Мухаммад Харид Растум // Конференция по исследованию права, компьютеров и Интернета в сотрудничестве с Центром стратегических исследований и разработок Эмиратов и Центром информационных технологий при университете: сборник. — Аль-Айн: Университет ОАЭ. Колледж шариата и права, 2004. — 1145 с. (на араб. яз.).

473. انوشا، سهیل، نیکجو، مهنوش، و کولیوند، روح اله. استراتژی امنیت سایبری. همایش ملی تحقیقات میان رشته ای در علوم مهندسی و مدیریت، ۱۴۰۰. [Сохаил Ануша, Махнуш Никджо, Рухолла Коливанда. Киберстратегия Ирана / Сохаил Ануша, Махнуш Никджо, Рухолла Коливанда // Междисциплинарные исследования, инженерные и управленческие науки: третья конференция. — Тегеран, 25.02.2022]. — URL: https://sid.ir/paper/902054/fa (дата обращения: 05.04.2025).

474. Tsyplakova A. Foreign Approaches to Droppers. III All-Russian Academic Hearings of Laws and Bills in the field of digital security. — MGIMO University, Irkutsk, 9 July of 2025. — URL: https://ssrn.com/abstract=5348975 (accessed 14.07.2025).

475. Tsyplakova A.D. Forms of Impact on Crime and their Significance. II International Scientific and Practical Conference ‘Strategies for Countering Crime in a Changing Reality’. — Sevastopol: the Law Institute of Sevastopol State University, 22 May of 2025. — URL: http://dx.doi.org/10.2139/ssrn.5248584 (accessed 14.07.2025).

Судебная практика

476. Raqib Hameed vs. Union of India represented by the Secretary Ministry of Electronics and Information Technology & Anr., W.P.(C) 5820/2024 // Delhi High Court: website. — URL: https://dhcappl.nic.in/dhcorderportal/GetOrder.do?ID=smp/2024/724909941714372150536_96365_58202024.pdf (accessed 02.05.2025).

477. Tanul Thakur vs. Union of India & Ors., W.P.(C) 13037/2019 // Delhi High Court: website. — URL: https://dhcappl.nic.in/dhcorderportal/GetOrder.do?ID=mmh/2022/1669727751905_9807_2022.pdf (accessed 02.05.2025).

478. Vijay Madanlal Choudhary and Others v. Union of India and Ors. (2022 SCC Online SC 929) // Supreme Court of Republic of India: website. — URL: https://scr.sci.gov.in/scrsearch/?p=pdf_search/home&text=Vijay%20Madanlal%20Choudhary&captcha=md7fMd&search_opt=PHRASE&fcourt_type=undefined&escr_flag=&

proximity=&sel_lang=&neu_cit_year=&neu_no=&ncn=&citation_vol=&citation_yr=&citation_supl=&citation_page=&app_token= (accessed 02.06.2025).

479. الطعن رقم ١٤٦٨ لسنة ٢٠٢٢ صادر بتاريخ ٢٠٢٣/٠٤/٢٥ [Апелляция No 1468 от 2022 года, по которой принято решение от 25.04.2023] // Официальная база законодательства ОАЭ: сайт. — URL: https://elaws.moj.gov.ae/UAE-MOJ_CP-Ar/00_2023/00_الجزائية%20الاحكام/UAE-CP-Ar_2023-04-25_01468_Taan.html (дата обращения: 19.03.2025).

480. ملف رقم: 1091284 قرار بتاريخ: 2022.01.13 [Номер файла: 1091284 Решение: 13.01.2022] // Верховный суд АНДР: официальный сайт. — URL: https://www.coursupreme.dz/-ملف-رقم-1091284-قرار-بتاريخ-20220113/الغرف-الجزائية/من-قرارات-المحكمة-العليا (дата обращения: 19.03.2025).

481. قرار الهيئة العامة للمحكمة العليا رقم (٣٤) وتاريخ ٢٤-٠٤-١٤٣٩هـ [Решение Генеральной Ассамблеи Верховного суда № 34 от 24.04.1439] // Юридическая контора Аль-Мухтара: сайт. — URL: https://elmokhtarlaw.com/-قرار-الهيئة-العامة-للمحكمة-العليا-رقم-3/ (дата обращения: 19.03.2025).

Энциклопедии, словари, справочники

482. Баранов Х.К. Большой арабско-русский словарь в 2-х томах. — Москва: Русский язык, 2006. — 1450 с. ISBN 978-5-91503-146-2.

483. Завадская Е.П. Учебный словарь новой лексики амхарского языка / Е.П. Завадская. — Москва: МГИМО-Университет, 2012. — 300 с. ISBN 978-5-9228-0671-8.

484. Иванов В.Б. Большой персидско-русский словарь: около 76000 слов, 61000 фразеологизмов и примеров: в трех томах. — Москва: Фонд Ибн Сины, 2023. — 1903 с.

485. Островенко Е.Д. Русско-персидский словарь дипломатической лексики: более 10 тысяч слов и словосочетаний на русском, персидском и дари языках. — 2-е издание, переработанное и дополненное. — Москва: МГИМО-Университет, 2020. — 698 с. ISBN 978-5-9228-2001-1.

486. Цифровой мир: терминологический словарь-справочник в определениях официальных документов / И. Р. Бегишев, И. Р. Альмухамедова, А. К. Арюков [и др.]. — Москва: Общество с ограниченной ответственностью «Проспект», 2024. — 672 с. ISBN 978-5-392-36024-6, 978-5-392-40409-4.

Официальные заявления представителей государственных органов

487. Egypt (30 June 2020) // UNODC: website. — URL: https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Comments/Egypt.pdf (accessed 20.04.2025).

488. Indonesia’s Submissions // UNODC: website. — URL: https://www.unodc.org/documents/Cybercrime/AdHocCommittee/First_session/Comments/Indonesias_input_AHC.pdf (accessed 21.04.2025).

489. India (23 August 2022) // UNODC: website. — URL: https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Second_intersessional_consultations/Revised_Indian_Text_for_UN_AHC_published_on_12.5.2022_-Revised_.pdf (accessed 20.04.2025).

490. Iran (Islamic Republic of) (20 April 2020) //UNODC: website. — URL: https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Comments/Iran.pdf (accessed 20.04.2025).

491. Islamic Republic of Iran (8 April 2022) // UNODC: website. — URL: https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Second_session/Islamic_Republic_of_Iran_contribution.pdf (accessed 20.04.2025).

492. Islamic Republic of Iran. Reconvened concluding session of the Ad Hoc Committee (29 July to 9 August 2024, New York) // UNODC: website. — URL: https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Reconvened_concluding_session/Written_submissions/MEMBER_STATES/Concept_note-comments-AHC.pdf (accessed 20.04.2025), Islamic Republic of Iran. Reconvened concluding session of the Ad Hoc Committee (29 July to 9 August 2024, New York) // UNODC: website. — URL: https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Reconvened_concluding_session/Written_submissions/MEMBER_STATES/I.R.Iran-_Statement_Ad_Hoc_Committee_30_July_2024_NY.pdf (accessed 20.04.2025).

493. Islamic Republic of Iran. Reconvened concluding session of the Ad Hoc Committee (29 July to 9 August 2024, New York) // UNODC: website. — URL: https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Reconvened_concluding_session/Written_submissions/MEMBER_STATES/I.R.Iran-Explanation_of_Position-9_August_2024_NY.pdf (accessed 20.04.2025).

494. Joint comment by Angola, Azerbaijan, Belarus, Burundi, Cambodia, China, Congo, Cuba, Democratic People's Republic of Korea, Eritrea, Ethiopia, Iran (Islamic Republic of), Kazakhstan, Kyrgyzstan, Lao People's Democratic Republic, Madagascar, Myanmar, Nicaragua, Pakistan, Russian Federation, Sudan, Suriname, Syrian Arab Republic, Tajikistan, Togo, Venezuela (Bolivarian Republic of) and Zimbabwe (9 February 2021) // UNODC: website. — URL: https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Comments/RF_9_February_2021.pdf pdf (accessed 20.04.2025).

495. Kuwait (17 September 2021) // UNODC: website. — URL: https://www.unodc.org/documents/Cybercrime/AdHocCommittee/First_session/Comments/Oman_18_Oct_2021.pdf (accessed 21.04.2025).

496. Oman (18 October 2021) // UNODC: website. — URL: https://www.unodc.org/documents/Cybercrime/AdHocCommittee/First_session/PM.SK.cm.166.2021.pdf (accessed 21.04.2025).

497. Russian Federation (27 May 2020) // UNODC: website. — URL: https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Comments/Russian_Federation.pdf (accessed 20.04.2025).

498. Statement of ASEAN and the Russian Federation on Cooperation against Illicit Drugs Trafficking // ASEAN: website. — URL: https://asean.org/wp-content/uploads/2021/10/81.-ASEAN-Russia-Statement-on-Drug-Cooperation-Final.pdf (accessed 26.04.2025).

499. UN Ad Hoc Committee (AHC) to elaborate a comprehensive International Convention on countering the use of Information and Communications Technologies for criminal purposes. Indian views on Scope, Objectives and Structure 6th December, 2021 // UNODC: website. — URL: https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Comments/India_-_Views_on_scope_objective_and_structure_7.12.2021_1.pdf (accessed 21.04.2025).

500. بيان وفد سلطنة عمان [Заявление делегации Султаната Оман] // УНП ООН: сайт. — URL: https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Reconvened_concluding_session/Written_submissions/MEMBER_STATES/_002.pdf (дата обращения: 21.04.2025).

501. عناصر ورقة من جانب جمهورية مصر العربية مقدمة الجلسة الثانية للجنة الخاصة (الأحكام العامة، التجريم، في مجال مكافحة استخدام تكنولوجيا الاتصالات والمعلومات لأغراض إجرامية بلورة اتفاقية دولية شاملة في إطار الأمم المتحدة [Элементы документа Арабской Республики Египет, представленного на второй сессии Специального комитета (Общие положения, криминализация, борьба с использованием ИКТ в преступных целях и разработка всеобъемлющей международной конвенции в рамках Организации Объединенных Наций)] // УНП ООН: сайт. — URL: https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Second_session/Egypt_contribution_A.pdf (дата обращения: 21.04.2025).

502. عناصر ورقة من جانب جمهورية مصر العربية مقدمة اتفاقية دولية شاملة في إطار الأمم المتحدة في إطار بلورة مكافحة استخدام تكنولوجيا الاتصالات والمعلومات لأغراض إجرامية [Элементы документа Арабской Республики Египет, представляющего всеобъемлющую международную конвенцию в рамках Организации Объединенных Наций по борьбе с использованием информационно-коммуникационных технологий в преступных целях] // УНП ООН: сайт. — URL: https://www.unodc.org/documents/Cybercrime/AdHocCommittee/First_session/Comments/Egypt_AHC_comments.pdf (дата обращения: 21.04.2025).

503. المملكة الأردنية الهاشمية اتفاقية شاملة بشأن مكافحة استخدام تكنولوجيا المعلومات والاتصالات للأغراض الإجرامية [Иорданское Хашимитское Королевство. «Всеобъемлющая конвенция о борьбе с использованием информационно-коммуникационных технологий в преступных целях»] // УНП ООН: сайт. — URL: https://www.unodc.org/documents/Cybercrime/AdHocCommittee/First_session/Comments/Jordan_AHC_Views_on_the_new_convention.pdf (дата обращения: 21.04.2025).

504. 中国对联合国打击为犯罪目的使用信通技术公约 范围 [Вклад Китая в Конвенцию Организации Объединенных Наций против использования ИКТ в преступных целях] // УНП ООН: сайт. — URL: https://www.unodc.org/documents/Cybercrime/AdHocCommittee/First_session/Comme

nts/Chinas_Suggestions_on_the_Scope_Objectives_and_Structure_AHC.pdf (дата обращения: 21.04.2025).

505. 中国关于网络空间国际规则的立场 [Позиция Китая по международным правилам киберпространства] // МИД КНР: сайт. — 2021. — URL: https://www.mfa.gov.cn/wjb_673085/zzjg_673183/jks_674633/zclc_674645/qt_674659/202110/t20211012_9552671.shtml (дата обращения: 07.07.2025).

Интернет-источники

506. Заместитель Генерального секретаря СНГ Н.Сейтимов принял участие в заседании Совета руководителей органов безопасности и специальных служб государств – участников СНГ // Интернет-портал СНГ. Пространство интеграции: сайт. — 16.05.2025. — URL: https://e-cis.info/news/564/127418/ (10.06.2025).

507. Игорь Краснов подписал с Генеральным прокурором Объединенных Арабских Эмиратов Хамадом Саифом Аль-Шамси дополнительный протокол о создании рабочей группы по противодействию преступности и защите прав граждан // Генеральная прокуратура: официальный сайт. — 15.04.2025. — URL: https://epp.genproc.gov.ru/web/gprf/mass-media/news?item=102347932 (дата обращения: 26.04.2025).

508. Проект ООН // УНП ООН: сайт. — URL: https://www.unodc.org/unodc/en/global-it-products/goaml.html (дата обращения: 16.05.2025).

509. African Union strengthens investigation capabilities on virtual assets and cybercrime // African Union: website. — 22.05.2024. — URL: https://au.int/ar/node/43809 (accessed 06.06.2025).

510. AI for Safer Children // UNICRI: website. — URL: https://unicri.org/topics/AI-for-Safer-Children (accessed 12.04.2025).

511. AlShatti Q. The launch of the Arab IGF // DiploFoundation: website. — 28.10.2013. — URL: https://www.diplomacy.edu/blog/launch-arab-igf/ (дата обращения: 12.06.2025).

512. Amrutha A. ATT(H)ack-Anti-Cyber Crime Law in Saudi Arabia // STA Law Firm: website. — 23.08.2017. — URL: https://www.stalawfirm.com/en/blogs/view/atthack-anti-cyber-crime-law-in-saudi-arabia.html (дата обращения: 09.03.2025).

513. AnJie Broad Law Firm. In brief: media law and regulation in China // Lexology: website. — 11.06.2024. — URL: https://www.lexology.com/library/detail.aspx?g=06005f86-e3e3-4106-8d55-736cf5da5e53 (accessed 19.05.2025).

514. Annual conference: 2022 // OIC-CERT: website. — URL: https://www.oic-cert.org/en/events/conference/2022.html (дата обращения: 25.03.2025).

515. ASEAN’s Cooperation on Cybersecurity and against Cybercrime. Presentation by the ASEAN Secretariat // Council of Europe: website. — 04.12.2013. —

URL: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802f2393 (accessed 20.05.2025).

516. Barakat W. How Dubai Police use AI to act on 'alarming' social media posts, protect children online // Khaleej Times: website. — 12.11.2024. — URL: https://www.khaleejtimes.com/business/tech/how-dubai-police-use-ai-to-act-on-alarming-social-media-posts-protect-children-online (accessed 12.05.2025).

517. Bug Bounty: official website. — Saudi Arabia. — URL: https://bugbounty.sa (accessed 25.03.2025).

518. China debates how to handle criminal crypto cache // Reuters: website. — 17.04.2025. — URL: https://www.reuters.com/world/china/china-debates-how-handle-criminal-crypto-cache-2025-04-15/ (accessed 22.05.2025).

519. Center For Cybercrime Investigation Training & Research // DSCI. URL: https://www.dsci.in/content/ccitr (accessed 08.04.2025).

520. China further regulates AI-generated content // Allen and Gledhill: website. — 02.04.2025. — URL: https://www.allenandgledhill.com/publication/articles/30284/further-regulates-ai-generated-content?agreed=cookiepolicy (accessed 19.05.2025).

521. China to Liquidate Seized Cryptocurrency Through Licensed Hong Kong Exchanges // Coinfea: website. — 07.06.2025. — URL: https://www.binance.com/en/square/post/25293712456530 (accessed 07.06.2025).

522. Crypto Crime Mid-Year Update // Chainalysis: website. — 08.2024. — URL: https://www.chainalysis.com/blog/2024-crypto-crime-mid-year-update-part-2/ (accessed 04.05.2025).

523. Cyber Crime Volunteer Program // Vijetha IAS Academy: website. — URL: https://vijethaiasacademy.com/blog/Cyber-Crime-Volunteer-Program (accessed 11.06.2025).

524. Cyber Drill // OIC CERT: website. — URL: https://www.oic-cert.org/en/events/cyber_drill/index.html (дата обращения: 25.03.2025).

525. CYBER JAAGROOKTA // I4C: website. — URL: https://i4c.mha.gov.in/cyber-jagrookta.aspx (accessed 25.03.2025).

526. CyberSouth // Council of Europe: website. — URL: https://rm.coe.int/3692-cybersouth-v13-extension-dec2021/1680a4d2a0 (accessed 06.06.2025).

527. CyberSouth+ // Council of Europe: website. — URL: https://rm.coe.int/3529-cybersouth-outline-en-v10-05-04-2024/1680af3217 (accessed 06.06.2025).

528. Dajani H. UAE to speed up criminal case processing by 100% using AI, blockchain // Khaleej Times: website. — 05.05.2025. — URL: https://www.khaleejtimes.com/uae/uae-speed-up-criminal-cases-ai-blockchain (accessed 12.05.2025).

529. Harris G. The State of Cyber Defense Cooperation in ASEAN // Real Clear Defense: website. — 31.01.2024. — URL: https://www.realcleardefense.com/articles/2024/01/31/the_state_of_cyber_defense_cooperation_in_asean_1008628.html (accessed 25.03.2025).

530. GCC Malware Analysis Platform Launched // Bahrain News Agency: website. — 20.07.2020. — URL: https://www.bna.bh/en/GCCMalwareAnalysisPlatformlaunched.aspx?cms=q8FmFJgiscL2fwIzON1%2BDtn0tM2%2FwwMJUBiBhb5CV%2Fc%3D (accessed 25.03.2025).

531. GLACY-e // Council of Europe: website. — URL: https://rm.coe.int/3399-glacy-e-summary-vfinal-en/1680ae1cba (accessed 06.06.2025).

532. Global Cybersecurity Index 2020 // ITU: website. — URL: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf (дата обращения: 09.03.2025).

533. Global Cybersecurity Index. 2024 // ITU: website. — URL: https://www.itu.int/dms_pub/itu-d/opb/hdb/d-hdb-gci.01-2024-pdf-e.pdf (дата обращения: 09.03.2025).

534. Information & eGovernment Authority Organizes First Cyber Drill for Cyber Hawks in Partnership with Kaspersky Lab // Kaspersky Lab: website. — 11.10.2017. — URL: https://me-en.kaspersky.com/about/press-releases/2017_information-egovernment-authority-organizes-first-cyber-drill (accessed 25.03.2025).

535. Isjchwansyah Y.R. Indonesia’s new cyber force needs to be planned, not rushed // ASPI: website. — 17.09.2024. — URL: https://www.aspistrategist.org.au/indonesias-new-cyber-force-needs-to-be-planned-not-rushed/ (accessed 25.03.2025).

536. Katte S. Scientists breach cryptographic algorithms with quantum computer: SCMP // Coin telegraph: website. — 14.10.2024. — URL: https://cointelegraph.com/news/scientists-breach-crypto-algorithms-quantum-computer-report (accessed 06.06.2025).

537. Khalila A. Rejuvenasi KPK: Urgensi Pemberlakuan Rancangan Undang-Undang Perampasan Aset dengan Pendekatan In Rem dan Tinjauan Pendekatan Serupa pada Regulasi Unexplained Wealth di Australia [Обновление КПК: срочность принятия проекта закона о конфискации активов с подходом In Rem и рассмотрение аналогичного подхода к регулированию необъясненного богатства в Австралии] // Институт научных исследований Юридического факультета Университета Индонезии. — URL: https://lk2fhui.law.ui.ac.id/portfolio/rejuvenasi-kpk-urgensi-pemberlakuan-rancangan-undang-undang-perampasan-aset-dengan-pendekatan-in-rem-dan-tinjauan-pendekatan-serupa-pada-regulasi-unexplained-wealth-di-australia/ (дата обращения: 02.06.2025).

538. Key Documents // ASEAN: website. — URL: https://asean.org/our-communities/economic-community/asean-digital-sector/ (accessed 03.05.2025).

539. Kovacs E. DeepSeek's Malware-Generation Capabilities Put to Test // Security Week: website. — 13.03.2025. — URL: https://www.securityweek.com/deepseeks-malware-generation-capabilities-put-to-test/ (accessed 12.06.2025).

540. Latest Documents // AU: website. — URL: https://au.int/documents/69 (accessed 04.05.2025).

541. List of Nodal Officers from States of India under the provisions of Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009 // Ministry of Electronics and Information Technology, Government of India: website. — URL: https://www.meity.gov.in/static/uploads/2024/12/ec8bee89ce950acd9ad5920c074146e7.pdf (accessed 02.05.2025).

542. List of Nodal Officers from Ministries/Departments of Central Government under the provisions of Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009 // Ministry of Electronics and Information Technology, Government of India: website. — URL: https://www.meity.gov.in/static/uploads/2024/12/b67f3564f0dc9df27f5eed565b600ce8.pdf (accessed 02.05.2025).

543. Major Sectoral Bodies/Committees // ASEAN: website. — URL: https://asean.org/our-communities/economic-community/asean-digital-sector/ (accessed 03.05.2025).

544. Maor E. AI Giving Rise of the 'Zero-Knowledge' Threat Actor // Security Week: website. — 02.04.2025. — URL: https://www.securityweek.com/ai-giving-rise-of-the-zero-knowledge-threat-actor/ (accessed 12.06.2025).

545. MOROCCO AND THE UNITED ARAB EMIRATES HAVE SIGNED A MEMORANDUM OF UNDERSTANDING (MOU) WITH THE AIM OF ENHANCING THEIR COOPERATION IN CYBERSECURITY // DGSSI: website. — URL: https://www.dgssi.gov.ma/en/evenements/morocco-and-united-arab-emirates-have-signed-memorandum-understanding-mou-aim-enhancing (accessed 24.05.2025).

546. Morocco investigates major data breach allegedly by Algerian hackers // The Record: website. — 11.04.2025. — URL: https://therecord.media/morocco-investigates-breach-hackers-algeria (accessed 12.06.2025).

547. National Cyber Crime Reporting Portal: official website. — India. — URL: https://cybercrime.gov.in (accessed 11.06.2025).

548. National Cyber Security Agency Honors 125 Entities for Participating in 2022 STAR Drill // Qatar News Agency: website. — 29.06.2022. — URL: https://www.qna.org.qa/en/News-Area/News/2022-06/29/0052-national-cyber-security-agency-honors-125-entities-for-participating-in-2022-star-drill (accessed 25.03.2025).

549. NEOM 'fully under Saudi sovereignty, regulations,' says government official refuting inaccurate media reports // Arab news: website. — 16.05.2022. — URL:

https://www.arabnews.com/node/2082796/business-economy (дата обращения: 25.03.2025).

550. Qatar's New Legal Framework for Regulating Digital Content Creation // Mashael Al Sulaiti Law Firm: website. — 12.01.2025. — URL: https://www.mas.com.qa/news/qatars-new-legal-framework-for-regulating-digital-content-creation (accessed 02.05.2025).

551. Oman ITU-Arab Regional Cybersecurity Centre // ITU: website. — URL: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/Global-Partners/oman-itu-arab-regional-cybersecurity-centre.aspx (accessed 25.03.2025).

552. Our initiatives // Saudi Federation for cybersecurity, programming & drones: website. — URL: https://safcsp.org.sa/en/portfolio#section-HakathonHomthem (accessed 25.03.2025).

553. PCFC, Government of Ghana sign MoU to establish economic zone, digital incubator in Accra // WAM: website. — 02.06.2025. — URL: https://www.wam.ae/en/article/bjzgjpg-pcfc-government-ghana-sign-mou-establish-economic (accessed 02.06.2025).

554. Phillips T. “Electronic heroin”: China’s boot camps get tough on internet addicts // The Guardian: website. — 28.08.2017. — URL: http://www.theguardian.com/world/2017/aug/28/electronic-heroin-china-boot-camps-Internet-addicts (accessed 09.05.2025).

555. Pig Butchering Scams: What the Data Shows // TRM Labs: website. — 02.2023. — URL: https://www.trmlabs.com/post/pig-butchering-scams-what-the-data-shows (accessed 11.05.2025).

556. Press releases. The African Union Convenes The Second African Cybercrime Forum // African Union: website. — 08.06.2021. — URL: https://au.int/fr/node/40556 (accessed 06.06.2025).

557. Public Prosecution develops AI-supported work system // WAM: website. — 17.10.2024. — URL: https://www.wam.ae/en/article/b5q8wqe-public-prosecution-develops-ai-supported-work (accessed 02.06.2025).

558. SAUDI ARABIA: Rules Released for Kingdom’s First Special Economic Zone // HKTDC: website. — 07.04.2021. — URL: https://research.hktdc.com/en/article/NzE0ODY3Nzc2 (accessed 25.03.2025).

559. Saudi Arabia Regulatory Update: Four new special economic zones launched // Clyde&Co: website. — 27.04.2023. — URL: https://www.clydeco.com/en/insights/2023/04/saudi-arabia-regulatory-update-economic-zones (accessed 25.03.2025).

560. Saudi Arabia’s Cybersecurity Recognized as 2nd Best Globally // National Cybersecurity Agency of the Kingdom of Saudi Arabia: website. — 20.06.2023. — URL: https://nca.gov.sa/en/news?item=556 (accessed: 09.03.2025).

561. Seeger R. The New Battlefront: Cyber Security Across the GCC // Gulf International Forum: website. — URL: https://gulfif.org/the-new-battlefront-cyber-security-across-the-gcc/ (accessed 12.01.2025).

562. Singh V.V. 6,600 crore bitcoin scam: ED seizes 1.6 crore Dubai assets // The Times of India: website. — 20.02.2025. — URL: http://timesofindia.indiatimes.com/articleshow/118395033.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst (accessed 03.06.2025).

563. Spence N. UAE Cybersecurity Council holds virtual exercise ‘Cyber 193’ with 140 countries // Security Middle East Magazine: website. — 21.03.2022. — URL: https://www.securitymiddleeastmag.com/uae-cybersecurity-council-holds-virtual-exercise-cyber-193-with-140-countries/ (accessed 25.03.2025).

564. SCO members invited to join new AI cooperation plan // Digwatch: website. — 31.05.2025. — URL: https://dig.watch/updates/sco-members-invited-to-join-new-ai-cooperation-plan (accessed 12.06.2025).

565. The 10th Regional cybersecurity Arabic regional and OIC-CERT drill kicks off // Ministry of Transport, Communications and Information Technology of Sultanate of Oman: website. — 06.11.2022. — URL: https://mtcit.gov.om/ITAPortal/MediaCenter/NewsDetail.aspx?NID=81251 (accessed 25.03.2025).

566. The First African Forum on Cybercrime // African Union: website. — URL: https://au.int/en/newsevents/20181016/first-african-forum-cybercrime (accessed 06.06.2025).

567. The National Cybersecurity Authority launches the “National Program for Cyber Drills” // National Cybersecurity Authority of the Kingdom of Saudi Arabia: website. — 14.11.2022. — URL: https://nca.gov.sa/en/news?item=372 (accessed 25.03.2025).

568. UAE’s Criminal Case Processing to Be Enhanced With AI & Blockchain // Scene Now UAE: website. — 06.05.2025. — URL: https://cairoscene.com/buzz/uae-s-criminal-case-processing-to-be-enhanced-with-ai-blockchain (accessed 02.06.2025).

569. Various measures have been taken by the government to strengthen cyber security in the financial sector // PIB Dehli: website. — 18.03.2025. — URL: https://www.pib.gov.in/PressReleasePage.aspx?PRID=2112323 (дата обращения: 11.06.2025).

570. Williams S. “Electronic heroin” spawns Chinese internet addiction camps // VOA: website. — 25.08.2024. — URL: https://www.voanews.com/a/electronic-heroin-spawns-chinese-Internet-addiction-camps/2427495.html (accessed 09.05.2025)

571. إبراهيم العلبي. حرب سيبرانية.. هكذا تكافح دول الخليج الإرهاب إلكترونياً [Ибрагим Альби. "Кибервойна". Вот как страны Персидского залива борются с терроризмом в электронном виде] // Alkhaleej: сайт. — URL: https://alkhaleejonline.net/-علوم-وتكنولوجيا/حرب-سيبرانية-هكذا-تكافح-دول-الخليج-الإرهاب-إلكترونياً (дата обращения: 25.03.2025).

572. أكاديمية طويق [Тувэйк Академия]: официальный сайт. — Эр-Рияд, Королевство Саудовская Аравия. — URL: https://tuwaiq.edu.sa (дата обращения: 25.03.2025).

573. سايبرهب [Киберхаб]: официальный сайт. — Эр-Рияд, Королевство Саудовская Аравия. — URL: https://cyberhub.sa (дата обращения: 25.03.2025).

574. كودرهب [Кодерхаб]: официальный сайт. — Эр-Рияд, Королевство Саудовская Аравия. — URL: https://coderhub.sa (дата обращения: 25.03.2025).

575. السلامة السيبرانية والأمن الرقمي [Кибербезопасность и цифровая безопасность] // ОАЭ: сайт. — URL: https://u.ae/ar-ae/information-and-services/justice-safety-and-the-law/cyber-safety-and-digital-security (дата обращения: 13.07.2023).

576. إبراهيم محمد شاكر علي، مشعل بن أحمد الشريده. تسخير التكنولوجيا لخدمة القانون والقضاء والأفراد التقاضي الإلكترونيُّ ومنصة ناجز في المملكة العربيَّة السعوديَّة أنموذجًا [Ибрагим Мохаммед Шакер Али, Мешаль бин Ахмед Аш-Шарида. Использование технологий в интересах закона, судебной системы и частных лиц Электронный судебный процесс и платформа Najeez в Королевстве Саудовская Аравия в качестве модели] // Ассоциация юристов APE: сайт. — 09.11.2023. — URL: https://egyls.com/تسخير-التكنولوجيا-لخدمة-القانون-والق/ (дата обращения: 02.05.2025).

577. الهيئة الوطنية للأمن السيبراني تشارك في تمرين افتراضي بحضور 25 دولة عربية وإقليمية [Национальное управление по кибербезопасности участвует в виртуальных учениях в присутствии 25 арабских и региональных стран] // Национальный центр безопасности КСА: сайт. — URL: https://cert.gov.sa/ar/media-center/news/cyber-drill-2020/ (дата обращения: 25.03.2025).

578. وزارة التقنية والاتصالات تشارك في اجتماع اللجنة التنفيذية للحكومة الإلكترونية ولجنة وكلاء البريد والاتصالات بدول مجلس التعاون لدول الخليج العربية [Министерство технологий и коммуникаций участвует в заседании Исполнительного комитета электронного правительства и комитета почтовых и телекоммуникационных агентств в государствах Персидского залива] // Oman News Agency: сайт. — URL: https://omannews.gov.om/topics/ar/112/show/378724 (дата обращения: 02.09.2023).

579. انعقاد أول اجتماع للجنة الخليجية للأمن السيبراني بالإمارات [Первое заседание Комитета по кибербезопасности Персидского залива в ОАЭ] // Alkhaleej: сайт. — URL: https://alkhaleejonline.net/علوم-وتكنولوجيا/انعقاد-أول-اجتماع-للجنة-الخليجية-للأمن-السيبراني-بالإمارات (дата обращения: 25.03.2025).

580. خلال انعقاد الاجتماع الأول للجنة الوزارية للأمن السيبراني بدول مجلس التعاون ... إطلاق التمرين الخليجي الأول للأمن السيبراني [Во время первого заседания Министерского комитета по кибербезопасности в странах Персидского залива ... Запуск первых учений по кибербезопасности в Персидском заливе] // Генеральный секретариат ССАГПЗ: сайт. — URL: https://www.gcc-sg.org/ar-sa/MediaCenter/NewsCooperation/News/Pages/news2022-10-23-4.aspx (дата обращения: 25.03.2025).

581. أهداف برنامج سفراء السلامة المعلوماتية [Цели Программы послов информационной безопасности] // Национальный центр информационной безопасности Султаната Оман: сайт. — URL: https://ambassadors.cert.gov.om/about_ar.aspx (дата обращения: 13.07.2023).

582. مفهوم الجرائم الإلكترونية [Концепция электронных преступлений] // Главное управление по борьбе с коррупцией и по экономической и электронной безопасности Королевства Бахрейн: сайт. — URL: https://www.acees.gov.bh/cyber-crime/the-concept-of-e-crimes/ (дата обращения: 09.03.2025).

583. الإمارات - 02/02/1446هـ الموافق 06/08/2024 م - شرطة أبوظبي تحذر الجمهور من طرق وأساليب الاحتيال المتجددة [ОАЭ 1446/02/02 АН соответствует 06/08/2024 AD - Полиция Абу-Даби предупреждает общественность о возобновляемых методах и методах мошенничества] // Совет арабских министров внутренних дел Лиги арабских государств: сайт. — URL: https://www.aim-council.org/awareness-programs/cybercrime-posters/52783/ (дата обращения: 10.05.2025).

584. اللجنة الوزارية للحكومة الالكترونية بدول مجلس التعاون تعقد اجتماعها الخامس في البحرين [Комитет министров электронного правительства стран Персидского залива проводит свое пятое заседание в Бахрейне] // Исполнительный комитет электронного правительства ССАГПЗ: сайт. — 21.03.2017. — URL: http://www.gcc-egov.org/ar/news_details?id=758559 (дата обращения: 25.03.2025).

585. شموس [Шумуусун] // Министерство внутренних дел КСА: сайт. — URL: https://www.moi.gov.sa/wps/portal/Home/sectors/publicsecurity/publicsecurity/shomoos/ (дата обращения: 19.06.2025).

586. «الداخلية» تؤكد الوصول لـ 70 ألف مطلوب ومخالف عبر «نظام شموس» [Министерство внутренних дел подтверждает прибытие 70 тысяч разыскиваемых и нарушителей через систему Шумуусун] // Новости «عكاظ»: сайт. — 14.05.2013. — URL: https://www.okaz.com.sa/article/570285/الداخلية-تؤكد-الوصول-ل-70-ألف-مطلوب-ومخالف-عبر-نظام-شموس (дата обращения: 19.06.2025).

587. الخليجي للأمن السيبراني يوصي باستراتيجية موحدة لمتابعة الجرائم الإلكترونية [«Gulf Cybersecurity» рекомендует единую стратегию по борьбе с киберпреступностью] // Aljarida: сайт. — 15.03.2023. — URL: https://www.aljarida.com/article/17840 (дата обращения: 25.03.2025).

588. تقرير لجنة الشؤون التشريعية والقانونية بخصوص الاقتراح بقانون بتنظيم تقنيات الذكاء الاصطناعي واستخداماته، والمقدم من أصحاب السعادة الأعضاء: علي حسين الشهابي، وجمال محمد فخرو، والدكتورة جهاد عبدالله الفاضل، والدكتور محمد علي حسن علي، ودلال جاسم الزايد [Доклад Комитета по законодательным и правовым вопросам относительно предлагаемого закона о регулировании технологий искусственного интеллекта и их использования, представленный членами: Али Хусейном Аль-Шехаби, Джамалом Мухаммадом Фахро, доктором Джихадом Абдуллой Аль-Фадилом, доктором Мохаммедом Али Хасаном Али и Далалом Джассимом Аль-Зайедом] // Комитет по законодательным и правовым вопросам Маджлис Аш-Шура Королевства Бахрейн: сайт. — URL: https://councilsessions-s3-bucket.s3.me-south-1.amazonaws.com/s28_06a_pdf-

1714037459122.pdf?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIA4XAHVY3LHQ7YI5EO%2F20240929%2Fme-south-1%2Fs3%2Faws4_request&X-Amz-Date=20240929T150137Z&X-Amz-Expires=900&X-Amz-Signature=6638b015b246846cd3a70da306bc21b72a43f3a95a0022a61a553bb0172eec3b&X-Amz-SignedHeaders=host (дата обращения: 25.03.2025).

589. اختبار الجاهزية الوطنية [Национальный текст готовности] // Национальный центр по кибербезопасности Королевства Бахрейн: сайт. — URL: https://www.ncsc.gov.bh/ar/programs-initiatives/national-cyber-capabilities/national-cyber-drill.html (дата обращения: 25.03.2025).

590. مبادرة التمارين السيبرانية للقطاعات الحيوية [Национальная инициатива по киберучениям в секторах] // Национальный центр по кибербезопасности Королевства Бахрейн: сайт. — URL: https://www.ncsc.gov.bh/ar/programs-initiatives/national-cyber-capabilities/sectoral-cyber-drill.html (дата обращения: 25.03.2025).

591. التوعية الأمنية [Повысить осведомлённость] // Национальный центр безопасности КСА: сайт. — URL: https://cert.gov.sa/ar/awareness/?page=1 (дата обращения: 25.03.2025).

592. سطر [Линия]: официальный сайт. — Эр-Рияд, Королевство Саудовская Аравия.— URL: https://satr.codes (дата обращения: 25.03.2025).

593. استقبلت وزارة التربية والتعليم وفد يضم عددًا من المختصين بمجال أمن المعلومات في دول مجلس التعاون الخليجي، بحضور سعادة الأستاذ الدكتور عبدالله بن خميس أمبوسعيدي وكيل الوزارة للتعليم، وذلك بقاعة نزوى بديوان عام الوزارة، وتأتي هذه الزيارة في إطار إبراز جهود أمن المعلومات التعليمية في الوزارة. [Министерство образования приняло делегацию, включающую ряд специалистов в области информационной безопасности в странах Совета сотрудничества залива, в присутствии заместителя министра образования Абдуллы бин Хамиса Амбусаиди в зале Низва главного офиса министерства, и этот визит проходит в рамках освещения усилий министерства по обеспечению информационной безопасности в сфере образования] // Educational Portal: сайт. — 25.08.2023. — URL: https://home.moe.gov.om/region/alwesta/topics/1/show/9843 (дата обращения: 25.03.2025).

594. حاضنة الأعمال الرقمية [Цифровой инновационный центр]: официальный сайт. — Доха, Катар. — URL: https://dic.mcit.gov.qa/ar/ (дата обращения: 12.06.2025).

595. القمة العربية الدولية للأمن السيبراني [Арабский саммит по кибербезопасности] // Управление информации и электронного правительства Королевства Бахрейн: сайт. — URL: https://www.iga.gov.bh/article/arab-international-cybersecurity-summit (дата обращения: 25.03.2025).

596. التوقيع على اتفاقية شراكة تهدف إلى إنشاء مركز للإبتكار في الأمن السيبراني [Подписание соглашения о партнерстве по созданию центра инноваций в области кибербезопасности] // Maacoom: сайт. — 31.05.2024. — URL:

https://maacom.ma/2024/05/31/التوقيع-على-اتفاقية-شراكة-تهدف-إلى-إنش/ (дата обращения: 12.06.2025).

597. الإدارة العامة للمباحث الجنائية [Главное управление уголовных расследований] // Министерство внутренних дел Государства Катар: сайт. — URL: https://portal.moi.gov.qa/wps/portal/MOIInternet/departmentcommittees/gacriminalinvestigation (дата обращения: 17.01.2025).

598. إدارة مكافحة الجرائم الإلكترونية [Департамент по борьбе с электронной преступностью] // Министерство внутренних дел Государства Кувейт: сайт. — URL: https://www.moi.gov.kw/main/sections/cyber-crime (дата обращения: 17.01.2025).

599. المغرب يمهد لإقامة "مركز سيبراني" [Марокко прокладывает путь к созданию «киберцентра»] // Hespress: сайт. — 01.06.2025. — URL: https://www.hespress.com/1569153-المغرب-يمهد-لإقامة-مركز-سيبراني.html (дата обращения: 12.06.2025).

600. 检察机关打击治理电信网络诈骗及其关联犯罪工 作 情 （2023 年） [Procuratorial Organs’ Efforts to Combat and Govern Telecommunications Network Fraud and Related Crimes (2023)] // Supreme People’s Procuratorate of the People’s Republic of China: website. — 30.11.2023. — URL: https://www.spp.gov.cn/xwfbh/wsfbt/202311/t20231130_635181.shtml#2 (accessed 11.05.2025).

601. 个人信息保护写进快板书 [Защита персональных данных записана в книге с хлопушкой] // Газета «People Daily»: сайт. — 01.11.2024. — URL: http://society.people.com.cn/n1/2024/1101/c1008-40351843.html (дата обращения: 06.06.2025).

602. 電腦 / 網絡犯罪 [Computer / Cybercrimes] // Polícia Judiciária do Governo da Região Administrativa Especial de Macau: website. — URL: https://www.pj.gov.mo/Web//Policia/law/?lang=en (accessed 06.06.2025).

603. 網絡安全及科技罪案 [Cyber Security and Technology Crimes] // Hong Kong Police Force: website. — URL: https://www.police.gov.hk/ppp_tc/04_crime_matters/tcd/legislation.html (accessed 06.06.2025).

604. 35% rise in cyber crimes in Q1 2025: ROP // Muscat Daily: website. — 26.05.2025. — URL: https://www.muscatdaily.com/2025/05/26/35-rise-in-cyber-fraud-crimes-in-q1-2025-rop/ (accessed 12.06.2025).

Аудиоматериалы

605. سلطنة عُمان ـ 03/06/1445هـ الموافق 16/12/2023م - أهم أساليب الاحتيال الإلكتروني الحديثة [Султанат Омана 1445/06/03 АН соответствует 16/12/2023 г. н.э. - Наиболее важные методы современного электронного мошенничества.]. Аудиозапись: электронная // Совет арабских министров внутренних дел Лиги арабских государств: сайт. —

URL: https://www.aim-council.org/awareness-programs/cybercrime-videos/50276/ (дата обращения: 10.05.2025).

Приложение № 1. Сравнение аутентичных наименований киберпреступлений с авторским переводом на русский язык

№	Язык	Наименование киберпреступления на государственном языке (аутентичный текст)	Наименование киберпреступления на английском языке (официальный текст)	Наименование киберпреступления на русском языке (авторский перевод с государственного языка)
1.1	**Арабский язык**	الجرائمُ الإلكترونيةُ	Cybercrimes	Электронные преступления
1.2		الجرائمُ المعلوماتيةُ	Cybercrimes	Информационные преступления
1.3		جرائمُ المعلوماتيةِ	Cybercrimes	Преступления в сфере информатики
1.4		جرائمُ تقنيةِ المعلوماتِ	Cybercrimes; Information Technology Crimes	Преступления в сфере информационных технологий
1.5		الجرائم المتصلة بتكنولوجيات الإعلام والإتصال	Information Technology Crimes	Преступления, связанные с информационно-коммуникационными технологиями
1.6		الجرائم المتصلة بأنظمة المعلومات والاتصال	Information Technology Crimes	Преступления, связанные с информационно-коммуникационными системами
1.7		الجرائم المتعلقة بالتجهيزات الحساسة	—	Преступления, связанные с чувствительным оборудованием
1.8		جرائم المساس بأنظمة المعالجة الآللية للمعطيات	Attacks on Automated Data Processing Systems	Преступления, связанные с автоматизированными системами обработки данных
1.9		الجرائم السيبرانية	Cybercrime	Киберпреступления
1.10		جرائم الحاسب الآلي	Computer crimes	Компьютерные преступления
2.1	**Персидский язык (фарси)**	جرائم رایانه ای	Cybercrime; Computer crimes	Компьютерные преступления
2.2		جرایم سایبری	Cybercrimes	Киберпреступления
3.1	**Амхарский язык**	የኮምፒዩተር ወንጀልን	Computer crimes	Компьютерные преступления
4.1	**Китайский язык (традиционный /**	网络违法犯罪 (网络犯罪)	Cybercrimes	Сетевые преступления
4.2		電腦 / 網絡犯罪	Computer / cybercrimes	Компьютерые / сетевые преступления

4.3	**упрощенный / тайваньский)**	科技罪案 (*упрощенный*)	Technology Crimes	Преступления в сфере технологий
4.4		電腦犯罪 (*тайваньский*)	Computer crimes	Компьютерные преступления
5.1	**Индонезийский язык**	Pidana di bidang Teknologi Informasi dan Transaksi Elektronik	—	Преступления в сфере информационных технологий и электронных транзакций
5.2		Tindak Pidana terhadap Informatika dan Elektronika		Преступления против информатики и электроники
6.1	**Французский язык[632]**	Cybercriminalité	—	Киберпреступления
7.1	**Португальский язык**	criminalidade informática	—	Информационное преступление

Таблица составлена автором

[632] Несмотря на то, что официальным языком Туниса, Марокко и АНДР является арабский, законодательство также публикуется и на французском языке.

Приложение № 2. Сравнение аутентичных наименований нормативных правовых актов отдельных стран Глобального Юга с официальными переводами на английский язык и авторским переводом на русский язык[633]

№	Государство	Наименование нормативно-правового акта на иностранном языке (официальный текст)	Наименование нормативно-правового акта на русском языке (авторский перевод с иностранного языка)	Наименование нормативно-правового акта на английском / португальском языке (официальный текст)
1.1	**Королевство Саудовская Аравия**	نظام مكافحة جرائم المعلوماتية ١٤٢٨	Положение от 27.03.2007 «О борьбе с преступлениями в сфере информатики»	Anti-Cyber Crime Law 1428 H
1.2		نظام التعاملات الإلكترونية ١٤٢٨	Положение от 27.03.2007 Об электронных сделках»	Electronic Transactions Law 1428 H
1.3		نظام المطبوعات والنشر	Положение от 02.04.2000 «О печати и публикациях»	Printing and Publication Law
1.4		نظام حماية البيانات الشخصية	Положение от 16.09.2021 «О защите персональных данных»	—
1.5		نظام التجارة الإلكترونية	Положение от 10.07.2019 «Об электронной торговле»	E-Commerce Law

[633] Перечень нормативных правовых актов не является исчерпывающим, не содержит антитеррористических, общеуголовных и уголовно-процессуальных законов.

2.1	**Объединённые Арабские Эмираты**	مرسوم بقانون اتحادي رقم ٣٤ لسنة ٢٠٢١ في شأن مكافحة الشائعات والجرائم الإلكترونية	Федеральный декрет-закон № 34 2021 года «О борьбе со слухами и электронными преступлениями»	Federal Decree Law No. 34 of 2021 on Combatting Rumours and Cybercrimes
2.2		مرسوم بقانون اتحادي رقم ٤٦ لسنة ٢٠٢١ بشأن المعاملات الإلكترونية وخدمات الثقة	Федеральный декрет-закон № 46 2021 года «Об электронных транзакциях и трастовых услугах»	Federal Decree Law No. 46 of 2021 on Electronic Transactions and Trust Services
2.3		المرسوم بقانون اتحادي رقم ٤٥ لسنة ٢٠٢١ بشأن حماية البيانات الشخصية	Федеральный Декрет-закон № 45 2021 года «О защите персональных данных»	Federal Decree Law No 45 of 2021 regarding the Protection of Personal Data
2.4		مرسوم بقانون اتحادي رقم ٢ صادر بتاريخ ٢٠١٥ في شأن مكافحة التمييز والكراهية	Федеральный Декрет-Закон № 2 2015 года «О борьбе с дискриминацией и ненавистью»	Federal Decree Law No. 2 of 2015 on Combating Discrimination and Hatred
2.5		لائحة تنظيم استخدام موظفي الجهات الاتحادية لوسائل التواصل الاجتماعي المعتمدة بقرار مجلس الوزراء رقم (3/73و/1) لسنة 2014	Решение Совета министров № 1/у73/3 от 2014 года «О регулировании использования социальных сетей сотрудниками федеральных органов власти»	Cabinet Resolution No. 73/3/&1 of 2014 Regulation of Using Social Media by the Employees of Federal Entities
2.6		القرار الوزاري رقم (1) لسنة 2008 في شأن إصدار لائحة مزودي خدمات التصديق الإلكتروني	Решение министра № 1 от 2008 года «Регулирование поставщика сертификационных услуг»	Ministerial Resolution No. 1 of 2008 Regarding the issuance of Certification Service Provider Regulations

2.7		قانون تنظيم نشر وتبادل البيانات في إمارة دبي	Закон № 26 от 2015 года, регулирующий распространение и обмен данными в эмирате Дубай	Law No. 26 of 2015 Regulating Data Dissemination and Exchange in the emirate of Dubai
2.8		قانون اتحادي رقم ١٥ في شأن المطبوعات والنشر	Федеральный закон № 15 от 16.11.1980 «О публикациях и издании»	Federal Law No. 15 issued on 1980/11/16 corresponding to 8 Muharram 1401 H. Concerning Publications and Publishing
2.9		قرار مجلس الوزراء رقم ٢٨ لسنة ٢٠٢٣ بشأن الائحة التنفيذية للمرسوم بقانون اتحادي رقم ٤٦ لسنة ٢٠٢١ بشأن العاملات الإلكترونية وخدمات الثقة	Решение Совета министров № 28 от 19.05.2023 «Исполнительный регламент Федерального закона-декрета № 46 от 2021 года «Об электронных трансакциях и трастовых услугах»	Cabinet Resolution No. (28) for 2023 on the Executive Regulations of Federal Law by Decree No. (46) of 2021 on electronic Transactions and Trust Services
2.10		مرسوم بقانون اتحادي رقم (3) لسنة 2003 في شأن تنظيم قطاع الاتصالات	Федеральный декрет-закон № 3 от 14.04.2003 «О регулировании телекоммуникационного сектора»	—
2.11		قرار وزاري رقم ٨٦ صادر بتاريخ ٢٠٢٠/٢/٢ بشأن ضوابط أمن المعلومات بوزارة العدل والتزامات المستخدمين	Решение министра № 86 от 02.02.2020 «О контроле информационной безопасности в Министерстве юстиции и обязательствах пользователей»	—

2.12		قرار مجلس الوزراء رقم ٢١ صادر بتاريخ ٢٠١٣/٠٧/٠٣م بشأن لائحة أمن المعلومات في الجهات الاتحادية	Постановление Совета Министров № 21 от 07.03.2013 «О регулировании информационной безопасности в федеральных органах»	—
2.13		قانون اتحادي رقم (2) لسنة 2019 في شأن استخدام تقنية المعلومات والاتصالات في المجالات الصحية	Федеральный закон № 2 от 2019 года «Об использовании информационно-телекоммуникационных технологий в сфере здравоохранения»	—
2.14		مرسوم بقانون اتحادي رقم (38) لسنة 2021 بشأن حقوق المؤلف والحقوق المجاورة	Федеральный декрет-закон № 38 от 2021 года «Об авторском праве и смежных правах»	Federal Decree-Law no. (38) of 2021 on copyrights and neigbouring rights
2.15		قرار مجلس الوزراء رقم ١١١ صادر بتاريخ 2022/12/12م بشأن تنظيم الأصول الافتراضية ومزودي خدماتها	Постановление Совета министров № 111 от 22.12.2022 «О регулировании виртуальных активов и поставщиков услуг»	—
2.16		قانون رقم ١٤ لسنة ٢٠٢٣ بشأن التجارة من خلال وسائل التقنية الحديثة	Федеральный декрет-закон № 14 от 2023 года «О торговле с помощью современных технологий»	Federal Decree-Law No. 14/2023 on Trading by Modern Technological Means
2.17		قانون اتحادي رقم (15) لسنة 2020 في شأن حماية المستهلك	Федеральный закон № 15 от 2020 года «О защите потребителей»	Federal Law No (15) of 2020 on Consumer Protection

2.18		قرار مجلس الوزراء رقم (66) لسنة 2023 بشأن اللائحة التنفيذية للقانون الاتحادي رقم (15) لسنة 2020 في شأن حماية المستهلك	Постановление Совета министров № 66 от 2023 года «Исполнительный регламент к Федеральному закону № 15 от 2020 года «О защите потребителей»	Cabinet Decision No. 66 of 2023 issuing the highly anticipated Executive Regulations of the Consumer Protection Law
3.1	**Государство Катар**	قانون رقم ١٤ لسنة ٢٠١٤ بإصدار قانون مكافحة الجرائم الإلكترونية	Закон № 14 от 02.10.2014 «О борьбе с электронными преступлениями»	Law No. 14 of 2014 Promulgating Cybercrime Prevention Law
3.2		قانون رقم ١٣ لسنة ٢٠١٦ بشأن حماية خصوصية البيانات الشخصية	Закон № 13 от 29.12.2016 «О защите конфиденциальности персональных данных»	—
3.3		مرسوم بقانون رقم ١٦ لسنة ٢٠١٠ بإصدار قانون المعاملات والتجارة الالكترونية	Декрет-закон № 16 от 19.08.2010 «Об электронных транзакциях и электронной торговле»	Decree Law No. 16 of 2010 Promulgating the Electronic Transactions and Commerce Law
3.4		مرسوم بقانون رقم ٣٤ لسنة ٢٠٠٦ بإصدار قانون الاتصالات	Декрет-закон № 34 от 06.11.2006 «О связи»	Decree-Law No 34 of 2006 Promulgating the Telecommunications Law
4.1	**Султанат Оман**	مرســـوم سلطاني رقـم ٢٠١١/١٢ بإصدار قانون مكافحة جرائم تقنية المعلومات	Указ Султана № 12 2011 года «О борьбе с преступлениями в сфере информационных технологий»	Royal Decree No 12/2011 Issuing the Cybercrime Law
4.2		مرسوم سلطاني رقم ٢٠٠٨/٦٩ بإصدار القانون المعاملات الإلكترونية	Указ Султана Оман № 69 2008 года «Об электронных данных»	Royal Decree 69/2008 Issuing the Electronic Transactions Law of the Sultanate of Oman

4.3		مرسوم سلطاني رقم ٣٠ / ٢٠٠٢ بإصدار قانون تنظيم الاتصالات	Указ Султана № 30 2002 года «Об организации коммуникаций»	Telecommunications Regulatory Act
4.4		مرسوم سلطاني رقم ٦ / ٢٠٢٢ بإصدار قانون حماية البيانات الشخصية	Указ Султана № 6 2022 года «О персональных данных»	Royal Decree 6/2022 Promulgating the Personal Data Protection Law
4.5.		وزارة النقل والاتصالات وتقنية المعلومات: قرار وزاري رقم ٣٤ / ٢٠٢٤ بإصدار اللائحة التنفيذية لقانون حماية البيانات الشخصية	Решение Министра транспорта, связи и информационных технологий Султаната Оман № 34 от 28.01.2024 «Об исполнительном регламенте к Закону о персональных данных»	Ministry of transport, communications, and information technology: ministerial decision 34/2024 issuing the executive regulation of the personal data protection law
4.6		مرسوم سلطاني رقم ٥٨ / ٢٠٢٤ بإصدار قانون الإعلام	Указ Султана № 58 2024 года «О СМИ»	Royal Decree 58/2024 Issuing The Media Law
4.7		وزارة النقل والاتصالات وتقنية المعلومات: تعميم رقم ١١ / ٢٠٢٥ السياسة العامة للاستخدام الآمن والأخلاقي لأنظمة الذكاء الاصطناعي أبريل ٢٠٢٥م	Циркуляр Министерства транспорта, связи и информационных технологий № 11/2025 от 09.04.2025 «Общая политика безопасного и этического использования систем искусственного интеллекта»	Circular 11/2025 The Public Policy For The Safe And Ethical Use Of Artificial Intelligence Systems April 2025

5.1	**Государство Кувейт**	قانون رقم ٦٣ لسنة ٢٠١٥ في شأن مكافحة جرائم تقنية المعلومات	Закон № 63 2015 года «О борьбе с преступлениями в сфере информационных технологий»	Law No. (63) for the year 2015 on Combating Information Technology Crimes
5.2		قانون رقم ٣٧ لسنة ٢٠١٤ بإنشاء هيئة تنظيم الاتصالات وتقنية المعلومات	Закон № 37 2014 года «Об учреждению органа, регулирующего коммуникации и информационные технологии»	Law No. 37 of 2014 on the Establishment of Communication and Information Technology Regulatory Authority
6.1	**Королевство Бахрейн**	قانون رقم ٦٠ لسنة ٢٠٠٤ بشأن جرائم تقنية المعلومات	Закон № 60 2014 года «О преступлениях в области информационных технологий»	Law No. 60 of 2014 on Information Technology Crimes
6.2		مرسوم بقانون رقم ٥٤ لسنة ٢٠١٨ بإصدار قانون الخطابات والمعاملات الإلكترونية	Декрет-закон № 54 2018 года «Об электронных коммуникациях и сделках»	Legislative Decree No. (54) of 2018 Promulgating the Electronic Communications and Transactions Law
6.3		قانون رقم (30) لسنة 2018 بإصدار قانون حماية البيانات الشخصية	Закон № 30 2018 года «О защите персональных данных»	Law No. 30 of 2018 regarding Issuing the Protecting Personal Data law
6.4		مرسوم بقانون رقم (48) لسنة 2002 بإصدار قانون الاتصالات	Декрет-закон № 48 от 2002 года «О связи»	Legislative decree No. (48) of 2002 promulgating the telecommunications law

6.5		قرار رقم ٣٦ لسنة ٢٠١٨ بتنظيم الاشتراطات الفنية الخاصة بإرسال وتسَلُّم وتحديث السجلات والتوقيعات الإلكترونية للجهات العامة	Решение премьер-министра № 36 от 2018 года «О технических требованиях к отправке, получению и обновлению электронных записей и подписей органов публичной власти»	Decree of the Prime Minister No. 36 2018 regulating the technical requirements for sending, receiving, and updating the electronic records and signatures of the public bodies
7.1	**Арабская Республика Египет**	قانون مكافحة جرائم تقنية المعلومات رقم ١٧٥ لسنة ٢٠١٨	Закон АРЕ № 175 от 2018 года «О борьбе с преступлениями в сфере информационных технологий»	—
7.2		قانون رقم ١٥١ لسنة ٢٠٢٠ بإصدار قانون حماية البيانات الشخصية	Закон АРЕ № 151 2020 года «О защите персональных данных»	—
7.3		قانون تنظيم التوقيع الالكتروني وإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات رقم 15 لسنة 2004	Закон, регулирующий электронную подпись и учреждение Управления по развитию индустрии информационных технологий No 15 от 2004 года	—
8.1	**Королевство Марокко**	ظهير شريف رقم ١.٢٠.٦٩ صادر في ٤ ذي الحجة ١٤٤١ (٢٥) يوليو بتنفيذ القانون رقم ٠٥.٢٠ المتعلق بالأمن السيبراني	Королевский указ № 1.20.69, изданный 04.12.1441, соответствующий 25.07.2020 «Об издании закона № 05.20 касающегося кибербезопасности»	—

8.2		القانون رقم 08-09 المتعلق بحماية الأشخاص الذاتيين تجاه معالجة المعطيات ذات الطابع الشخصي	Закон № 08-09 «О защите физических лиц при обработке персональных данных» (Указ № 165-09-2 от 25 джумада I 1430 года (21 мая 2009 года))	—
8.3		القانون 03-07 المتمم لمجموعة القانون الجنائي فيما يتعلق بالجرائم المتعلقة بنظم المعالجة الآلية للمعطيات	Закон № 03-07 о дополнении Уголовного кодекса в части преступлений, связанных с автоматизированными системами обработки данных	—
8.4		القانون الموحد رقم 96-24 المتعلق بالبريد والمواصلات السلكية واللاسلكية	Единый закон № 96-24 о почте и телекоммуникациях	—
8.5		القانون رقم 08-31 القاضي بتحديد تدابير لحماية المستهلك، بما في ذلك حماية المستهلك على الإنترنت	Закон № 08-31 об установлении мер защиты прав потребителей, в том числе защиты прав потребителей в сети Интернет	—
8.6		القانون 05-53 المتعلق بالتبادل الإلكتروني للمعطيات القانونية	Закон № 05-53 об электронном обмене правовыми данными (Указ № 518-08-2 от 25 джумада I 1430 года (21 мая 2009 года))	—

8.7		القانون رقم 20-43 المتعلق بخدمات الثقة بشأن المعاملات الإلكترونية	Закон № 20-43 о трастовых услугах для электронных транзакций (Указ № 687-22-2, изданный 21 раби ас-сани 1444 года (16 ноября 2022 года))	—
8.8		مرسوم رقم 2.24.921 المتعلق بلجوء الهيئات والبنيات التحتية ذات الأهمية الحيوية المتوفرة على نظم معلومات حساسة أو معطيات حساسة إلى مقدمي الخدمات الرقمية السحابية	Указ № 2.24.921 о праве обращения жизненно важных организаций и инфраструктур с конфиденциальными информационными системами или конфиденциальными данными к поставщикам облачных цифровых услуг	—
8.9		مرسوم رقم 509-11-2 صادر في 22 شوال 1432 (21 شتنبر 2011) المتمم للمرسوم رقم 673-82-2 الصادر في 28 ربيع الأول 1403 (13 يناير 1983) المتعلق بتنظيم إدارة الدفاع الوطني و إحداث المديرية العامة لأمن نظم المعلومات	Указ № 509-11-2, изданный 22 шаввaля 1432 года (21 сентября 2011 года), вносящий поправки в Указ № 673-82-2, изданный 28 раби аль-авваля 1403 года (13 января 1983 года), регулирующий деятельность Национальной администрации обороны и создающий Главное управление безопасности информационных систем.	—

8.10		منشور رئيس الحكومة رقم 2023/2 الصادر في 12 يناير 2023 حول تطبيق التوجيهات الوطنية لأمن نظم المعلومات	Циркуляр премьер-министра № 2/2023 от 12 января 2023 года о внедрении Национальных директив по безопасности информационных систем	—
9.1	**Тунисская Республика**	مرسوم عدد 54 لسنة 2022 مؤرخ في 13 سبتمبر 2022 يتعلق بمكافحة الجرائم المتصلة بأنظمة المعلومات والاتصال	Указ № 54 от 13.09.2022 «О борьбе с преступлениями, связанными с информационно-коммуникационными системами»	—
9.2		المرسوم عدد 17 لسنة 2023 المتعلق بالسلامة السيبرنية	Указ № 17 от 2023 года «О кибербезопасности»	—
9.3		القانون الأساسي عدد 63 لسنة 2004 المؤرخ في 27 جويلية 2004 المتعلق بحماية المعطيات الشخصية	Органический закон № 63 от 27.07.2004 о защите персональных данных	—
9.4		الأمر عـدد 4773 لسنة 2014 مؤرخ في 26 ديسمبر 2014 يتعلق بضبط شروط وإجراءات إسناد ترخيص نشاط مزود خدمات الأنترنات	Приказ № 4773 от 26.12.2014 касается контроля условий и процедур назначения деятельности интернет-провайдера	—

9.5		الأمر حكومي عدد 417 لسنة 2018 مؤرخ في 11 ماي 2018 متعلق بإصدار القائمة الحصرية للأنشطة الاقتصادية الخاضعة لترخيص وقائمة التراخيص الإدارية لإنجاز مشروع وضبط الأحكام ذات الصلة وتبسيطها	Постановление Правительства № 417 от 11.05.2018 о выпуске исключительного перечня видов экономической деятельности, подлежащих лицензированию, и перечня административных лицензий для завершения проекта и контроля и упрощения соответствующих положений	—
9.6		قرار من وزير تكنولوجيات الاتصال والاقتصاد الرقمي ووزير التنمية والاستثمار والتعاون الدولي مؤرخ في 1 أكتوبر 2019 يتعلق بضبط كراس شروط ممارسة نشاط التدقيق في مجال السلامة المعلوماتية	Решение Министра коммуникационных технологий и цифровой экономики и Министра развития, инвестиций и международного сотрудничества от 01.10.2019 «Об утверждении Положения о порядке осуществления аудиторской деятельности в сфере обеспечения информационной безопасности»	—

9.7		قرار من وزير تكنولوجيات الاتصال مؤرخ في 13 سبتمبر 2023 يتعلق باجراءات وشروط إسناد وتجديد وسحب علامة "مسدي خدمات الحوسبة السحابية الحكومي" وعلامة "مسدي خدمات الحوسبة السحابية الوطني"	Решение Министра коммуникационных технологий от 13.09.2023 «О процедурах и условиях присвоения, продления и отзыва знака «Государственные услуги облачных вычислений» и «Национальный поставщик услуг облачных вычислений»	—
10.1	**Иорданское Хашимитское Королевство**	قانون الجرائم الإلكترونية رقم ١٧ لسنة ٢٠٢٣	Закон ИХК № 17 от 2023 года «Об электронных преступлениях»	—
10.2		قانون الاتصالات الأردني	Закон ИХК от 01.05.1995 «О СМИ»	—
10.3		قانون المعاملات الإلكترونية الأردني	Закон ИХК № 15 от 2015 г. «Об электронных коммуникациях»	—
10.4		قانون حماية البيانات الشخصية لسنة 2023	Закон ИХК от 2023 г. «О защите персональных данных»	—
10.5		تعليمات تحديد معايير مخالفات أحكام قانون الأمن السيبراني لسنة 2025	Инструкции по определению критериев нарушения положений Закона о кибербезопасности 2025 года	—
10.6		ظام ترخيص مقدمي خدمات الأمن السيبراني لسنة 2024	Закон о лицензировании поставщиков услуг в области кибербезопасности на 2024 год	—

10.7		تعليمات تصنيف حوادث الأمن السيبراني لسنة 2023	Инструкции по классификации инцидентов кибербезопасности на 2023 год	—
10.8		نظام المركز الوطني للأمن السيبراني لسنة 2020	Система Национального центра кибербезопасности на 2020 год	—
11.1	**الجزائر الديمقراطية الشعبية**	قانون رقم ٠٤-٠٩ مؤرخ في ١٤ شعبان عام ١٤٣٠ الموافق ٥ غشت سنة ٢٠٠٩، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها	Закон № 04-09 от 14.08.1430, соответствующий 05.08.2009, включающий специальные правила по предупреждению и борьбе с преступлениями, связанными с информационно-коммуникационными технологиями	—
11.2		قانون رقم ٠٧.٠٣ بتتميم مجموعة القانون الجنائي في ما يتعلق بالجرائم المتعلقة بنظم المعالجة الآلية للمعطيات	Закон № 07.03, дополняющий свод уголовного закона в части преступлений, связанных с автоматизированными системами обработки данных	—

11.3		القانون رقم 04-09 المؤرخ في 25 شعبان 1430 هـ الموافق 16 أغسطس 2009م يتضمن القواعد الخاصة للوقاية الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها	Закон № 04-09 от 25 шабан 1430 года хиджра, что соответствует 16 августа 2009 г. «Специальные правила по предупреждению и борьбе с преступлениями, связанными с информационно-коммуникационными технологиями»	—
12.1	**Исламская Республика Иран**	قانون جرائم رایانه ای	Закон ИРИ о компьютерных преступлениях	Computer Crimes Law
12.2		قانون تجارت الکترونیکی	Закон ИРИ об электронной коммерции	Electronic Commerce Law
12.3		قانون مطبوعات	Закон ИРИ о СМИ	Press Law
12.4		قانون نحوه مجازات اشخاصی که در امور سمعی و بصری فعالیت های غیرمجاز می نمایند	Закон ИРИ о порядке наказания лиц, осуществляющих несанкционированную деятельность в области аудиовизуальных дел	—
12.5		قانون مجازات استفاده کنندگان غیرمجاز از آب، برق، تلفن، فاضلاب و گاز	Закон ИРИ о наказании за несанкционированное пользование водой, электричеством, телефоном, канализацией и газом	—

13.1	**Федеративная Демократическая Республика Эфиопия**	አዋጅ ቁጥር ፱፻፶፰/ ፪ሺ፰ የኮምፒዩተር ወንጀልን ለመደንገግ የወጣ አዋጅ	Прокламация № 958 от 07.07.2016 «О компьютерных преступлениях»	Computer Crime Proclamation No. 958/2016
13.2		አዋጅ ቁጥር ፭ሺ፫፻፳፩/፪ሺ፲፮ የግል ዳታ ጥበቃን ለመደንገግ የወጣ አዋጅ	Прокламация № 1321 от 2024 г. «О безопасности персональных данных»	Proclamation No. 1321/2024 to provide for personal data protection
13.3		የኮምኒኬሽን አገልግሎት አዋጅ ቁ፭ሺ፻፺/፪ሺ፲፩	Прокламация № 1148 от 2019 г. «О коммуникационных услугах»	Proclamation No. 1148/2019 on Communications service
13.4		ሰለቴሌኮም ማጭበርበር ወንጀል የወጣ አዋጅ	Прокламация № 761 от 2012 г. «О телекоммуникационных мошенничествах»	Proclamation no. 761/2012 on telecom fraud offence
13.5		—	Прокламация № 590 от 2008 г. «О свободе СМИ и доступе к информации»	Proclamation No. 590/2008 to provide for freedom of the mass media and access to information
13.6		—	Прокламация № 1205 от 2020 г. «Об электронных транзакциях»	Proclamation No. 1205/2020 to provide for electronic transactions
13.7		—	Прокламация № 464 от 2005 г. «О защите телекоммуникационных и электрических сетей»	Proclamation No. 464/2005 to provide for the protection of telecommunication and electric power networks
13.8		—	Прокламация № 1072 от 2018 г. «Об электронной подписи»	Proclamation No. 1072/2018 to provide for electronic signature

13.9		አዋጅ ቁጥር ፭፻፭፻፲፰/፪፻፲፪ የጥላቻ ንግግርና የሐሰተኛ መረጃ ስርጭትን ለመከላከልና ለመቆጣጠር የወጣ አዋጅ	Прокламация № 1185 от 23.03.2020 «О предупреждении и пресечении разжигании ненависти и дезинформации»	Hate speech and disinformation prevention and suppression Proclamation No. 1185/2020
13.10		—	Прокламация № 759 от 27.08.2012 «О рекламе»	Proclamation No.759/2012 Advertisement Proclamation
13.11		—	Прокламаций ФДРЭ № 1284 от 18.04.2023 «Об эфиопской цифровой идентификации»	Proclamation No. 1284/2023 Ethiopian Digital Identification Proclamation
14.1.1	**Китайская Народная Республика**	关于办理信息网络犯罪案件适用刑事诉讼程序	Мнения Верховного народного суда КНР, Высшей народной прокуратуры КНР, Министерства общественной безопасности КНР от 26.08.2022 «По нескольким вопросам применения уголовных процедур при разрешении дел о преступлениях в информационных сетях»	—
14.1.2		最高检印发《人民检察院办理网络犯罪案件规定》	Уведомление Высшей народной прокуратуры КНР от 22.01.2021 «Об издании положений касательно сетевых преступлений, расследуемых народной прокуратурой»	—

14.1.3		中华人民共和国治安管理处罚法	Закон Китайской Народной Республики об административных штрафах за нарушение общественной безопасности	Public Security Administration Punishments Law of the People’s Republic of China
14.1.4		中华人民共和国网络安全法	Закон Китайской Народной Республики о сетевой безопасности	Cybersecurity Law of the People’s Republic of China
14.1.5		中华人民共和国反不正当竞争法	Закон Китайской Народной Республики о борьбе с недобросовестной конкуренцией	Anti-unfair Competition Law of the People’s Republic of China
14.1.6		网络安全审查办法	Меры по проверке сетевой безопасности	Measures for Cybersecurity Review
14.1.7		儿童个人信息网络保护规定	Положение о сетевой защите личной информации детей	Provisions on Protection of Children’s Personal Information Online
14.1.8		关键信息基础设施安全保护条例	Положение о защите безопасности критической информационной инфраструктуры	Regulations on the Security Protection of Critical Information Infrastructure
14.1.9		关于印发网络产品安全漏洞管理规定的通知	Положение об издании положений об управлении уязвимостями безопасности в сетевых продуктах	Provisions on the Management of Network Product Security Vulnerabilities
14.1.10		网络安全审查办法	Меры по обзору сетевой безопасности	Cybersecurity Review Measures

14.1.11		中華人民共和國數據安全法	Закон Китайской Народной Республики о безопасности данных	Data Security Law of the People's Republic of China
14.1.12		汽车数据安全管理若干规定	Административные положения об управлении безопасностью автомобильных данных	Administrative Provisions on the Security of Automobile Data
14.1.13		深圳经济特区数据条例	Положение о данных особой экономической зоны Шэньчжэнь	Regulations of Shenzhen Special Economic Zone on Data
14.1.14		中华人民共和国个人信息保护法	Закон Китайской Народной Республики о защите личной информации	Personal Information Protection Law of the People's Republic of China
14.1.15		促进和规范数据跨境流动规定	Положения о поощрении и регулировании трансграничного потока данных	Provisions on Promoting and Regulating Cross-border Data Flows
14.1.16		中华人民共和国密码法	Закон Китайской Народной Республики о криптографии	Cryptography Law of the People's Republic of China
14.1.17		中华人民共和国电子商务法	Закон Китайской Народной Республики об электронной коммерции	E-Commerce Law of the People's Republic of China
14.1.18		中华人民共和国电信条例	Положения о телекоммуникациях Китайской Народной Республики	Telecommunications Regulations of the People's Republic of China

14.1.19		政务数据共享条例	Правила совместного использования правительственных данных	Interim Measures for the Administration of Sharing of Government Information
14.2.1	**САР Макао**	網絡安全法	Закон о сетевой безопасности	Lei da cibersegurança
14.2.2		電信綱要法	Закон о телекоммуникациях	a Lei de Bases das Telecomunicações
14.2.3		電腦犯罪法	Закон о компьютерных преступлениях	Lei de combate à criminalidade informática
14.2.4		個人資料保護法	Закон о защите данных	a Lei da Protecção de Dados Pessoais
14.3.1	**САР Гонконг**	本条例旨在为电讯、电讯服务与电讯器具及设备的发牌和管制订定更完备的条文	Акт по обеспечению более совершенных положений по лицензированию и регулированию телекоммуникаций, телекоммуникационных услуг и телекоммуникационного оборудования и оборудования	An Ordinance to make better provision for the licensing and control of telecommunications, telecommunications services and telecommunications apparatus and equipment

14.3.2		本条例旨在管制内容属于或含有淫亵或不雅资料(包括暴力、腐化或可厌的资料)的物品，设立审裁处以裁定物品是否淫亵或不雅，或裁定公开展示的事物是否不雅，以及将物品评定为属淫亵、不雅或非淫亵亦非不雅的类别，并为附带事宜订定条文	Акт для контроля за предметами, содержание которых является или содержит непристойные или непристойные материалы (включая насильственные, коррумпированные или нежелательные материалы), создания трибунала для определения того, является ли предмет непристойным или непристойным, или является ли вещь, демонстрируемая в общественных местах, непристойной, а также классификации предмета как непристойный, неприличный или не непристойный и неприличный, а также вспомогательных вопросов	An Ordinance to control articles which consist of or contain material that is obscene or indecent (including material that is violent, depraved or repulsive), to establish tribunals to determine whether an article is obscene or indecent, or whether matter publicly displayed is indecent, and to classify articles as obscene or indecent or neither obscene nor indecent, and for matters incidental thereto

14.3.3		本条例旨在禁止儿童色情物品的生产、管有和发布；修订《刑事罪行条例》(第 200 章)，以禁止利用、促致或提供未满 18 岁的人以制作色情物品或作真人色情表演，扩大该条例某些性罪行条文的适用范围，使其扩及在香港以外地方对儿童作出的作为，并禁止作出关于该等作为的安排和禁止该等安排的广告宣传；以及就相关目的订定条文	Акт для запрета на производство, хранение и распространение детской порнографии; внесения поправок в Закон о преступлениях (глава 200) с целью запретить использование, приобретение или предоставление лиц моложе 18 лет для производства порнографических материалов или живых порнографических представлений, распространить применение некоторых положений Указа о сексуальных преступлениях на действия, совершенные в отношении детей за пределами Гонконга, а также запрета сговоров с такими действиями и запретить рекламу таких мероприятий; принятия мер для соответствующих целей	An Ordinance to prohibit the production, possession and publication of child pornography; to amend the Crimes Ordinance (Cap. 200) to prohibit the use, procurement or offer of persons under the age of 18 for making pornography or for live pornographic performances, to extend the application of certain sexual offence provisions of that Ordinance to acts committed against children outside Hong Kong, and to prohibit the making of arrangements relating to the commission of those acts and the advertisement of such arrangements; and to make provision for connected purposes

15.1	**Индонезийская Республика**	Peraturan Menteri Komunikasi dan Informatika Nomor 5 Tahun 2021 tentang Penyelenggaraan Telekomunikasi	решение Министра коммуникаций и информатики Республики Индонезия № 5 от 01.04.2021 «О внедрении телекоммуникаций»	—
15.2		Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik	Закон Республики Индонезия № 11 от 02.01.2024 «О внесении изменений в Закон № 11 2008 г. об электронной информации и транзакциях»	—
15.3		Undang-undang (UU) Nomor 27 Tahun 2022 Pelindungan Data Pribadi	Закон Республики Индонезия № 27 от 17.10.2022 «О защите персональных данных»	—
15.4		Peraturan Menteri Komunikasi dan Informatika Nomor 16 Tahun 2018. Ketentuan Operasional Sertifikasi Alat dan/atau Perangkat Telekomunikasi	решение Министра связи и информатики № 16 от 2018 г. Оперативные положения по сертификации телекоммуникационных средств и/или устройств	Regulation of the Minister of Communication and Informatics Number 16 of 2018 Operational Provisions for Certification of Telecommunication Tools and/or Devices
16.1	**Республика Индия**	—	Закон Республики Индия № 21 от 09.06.2000 «Об информационных технологиях»	Information Technology Act, 2000

16.2		—	Закон Республики Индия № 44 от 24.12.2023 «О телекоммуникациях»	Telecommunications Act 2023
16.3		—	Закон Республики Индия № 22 от 11.08.2023 «О защите цифровых персональных данных»	Digital Personal Data Protection Act 2023
16.4		—	Указания индийской	CERT-In directions under Section 70B
16.5		—	Информационно-технологические правила Республики Индия (Промежуточное руководство и Кодекс цифровых медиа) от 25.02.2021 (в ред. от 06.04.2023)	The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021
16.6		—	Правила информационных технологий (разумные методы и процедуры обеспечения безопасности и чувствительные персональные данные или информация) 2011 года	Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011 (SPDI Rules)

16.7		—	Правила информационных технологий (практика и процедуры обеспечения информационной безопасности для защищенной системы) 2018 г.	Information Technology (Information Security Practices and Procedures for Protected System) Rules 2018
16.8		—	Правила Aadhar (безопасность данных) 2016 г.	The Aadhar (Data Security) Regulations 2016
16.9		—	Политика Meghraj - лучшие практики облачной безопасности	Meghraj Policy – Cloud Security Best Practices
16.10		—	Национальная политика и руководство по информационной безопасности 2019 г.	National Information Security Policy and Guidelines 2019
16.11		—	Правила телекоммуникаций (критическая телекоммуникационная инфраструктура), выпущенные Министерством коммуникаций РИ от 22.11.2024	Telecommunications (Critical Telecommunication Infrastructure) Rules, 2024
16.12		—	Правила кибербезопасности телекоммуникаций от 2024 г.	Telecommunication Cyber Security Rules 2024

Таблица составлена автором

Приложение № 3. Сравнение законодательных видов киберпреступлений в отдельных странах Глобального Юга

№	Государство	Наименование киберпреступлений согласно нормативно-правовым актам	Законодательные виды киберпреступлений
1	**Королевство Саудовская Аравия**	Преступления в сфере информатики	—
2	**Объединённые Арабские Эмираты**	Электронные преступления	Преступления в сфере информационных технологий
			Преступления, связанные с контентом
			Преступления, связанные с распространением слухов и фэйковых новостей
3	**Государство Катар**	Электронные преступления + компьютерные (экономические) преступления	Подлог и электронное мошенничество
			Посягательства на информационные системы, программное обеспечение, информационные сети и электронные сайты
			Посягательства на права интеллектуальной собственности
			Преступления, связанные с электронными трансакциями
			Преступления, связанные с контентом
4	**Султанат Оман**	Преступления в сфере информационных технологий	Нарушение КЦД электронных данных, информации и информационной системы
			Преступления, связанные с контентом
			Незаконное использование финансовой карты

			Злоупотребление ИТ средствами
			Подлог и мошенничество в отношении информации
5	**Государство Кувейт**	Преступления в сфере информационных технологий	—
6	**Королевство Бахрейн**	Преступления в сфере информационных технологий	Преступления, связанные с ИТ и данными
			Преступления, связанные с ИТ средствами
			Преступления, связанные с контентом
7	**Арабская Республика Египет**	Преступления в сфере информационных технологий	Атаки на безопасность информационных сетей, систем и технологий
			Преступления, совершаемые с использованием информационных систем и технологий
			Преступления, связанные с посягательством на неприкосновенность частной жизни и незаконным информационным контентом
			Преступления, совершенные администратором веб-сайта
8	**Королевство Марокко**	Киберпреступления	—
9	**Тунисская Республика**	Преступления, связанные с информационно-коммуникационными системами	Нападение на целостность и конфиденциальность информационных систем и систем данных
			Преступления, совершенные с использованием информационных систем или данных
			Эксплуатация детей и физическое насилие
			Нарушение условий сбора электронных доказательств

10	**Иорданское Хашимитское Королевство**	Электронные преступления	—
11	**Алжирская Народная Демократическая Республика**	Преступления в сфере информационных технологий + Преступления, связанные с чувствительным оборудованием / АСОД	—
12	**Исламская Республика Иран**	Компьютерные преступления	Преступления против конфиденциальности данных, компьютерных и телекоммуникационных систем
			Преступления против целостности и неприкосновенности данных, компьютерных и телекоммуникационных систем
			Кража и мошенничество, связанные с компьютерами
			Преступления против целомудрия и общественной морали
			Клевета и публикация ложных сведений
			Иные
13	**Федеративная Демократическая Республика Эфиопия**	Компьютерные преступления	Преступления против компьютерной системы и компьютерных данных
			Деяния, связанные с подлогом, мошенничеством и кражей
			Нелегальный контент
			Иные

14.1	**Китайская Народная Республика**	Сетевые преступления	Случаи, угрожающие безопасности компьютерных информационных систем
			Случаи отказа от выполнения обязательств по управлению безопасностью информационных сетей, незаконного использования ИС или оказания помощи в преступной деятельности в ИС
			Случаи, когда информационные сети использовались для совершения основных преступлений, таких как мошенничество, азартные игры, нарушения в отношении персональных данных граждан
14.2	**САР Макао**	Компьютерные преступления	Незаконный доступ к компьютерной системе
			Незаконное получение, использование или доступность компьютерных данных
			Незаконный перехват компьютерных данных
			Повреждение компьютерных данных
			Препятствование работе компьютерной системы
			Компьютерные устройства или данные, предназначенные для совершения преступлений
			Использование компьютерного устройства для имитации станции мобильной связи
			Незаконное раскрытие серьезной уязвимости компьютерной безопасности
			Компьютерный подлог
			Компьютерное мошенничество
15	**Индонезийская Республика**	Преступления против информатики и электроники	—

16	**Республика Индия**	Кибер-преступления	—

Таблица составлена автором

Приложение № 4. Сравнение положений Будапештской, Арабской и Универсальной конвенций, а также Соглашения ШОС и Конвенции АС

Деяние	Будапештская конвенция	Соглашение ШОС	Арабская конвенция	Конвенция АС	Универсальная конвенция[634]
Незаконный доступ к компьютерной системе / ИТ	ст. 2: к компьютерной системе	Информационная преступность	ст. 6: к ИТ	п. 1 ст. 29: атаки на компьютерные системы	ст. 7: к ИКС
Неправомерные доступ, перехват или получение данных	ст. ст. 2, 3	Информационная преступность	ст. ст. 6, 7, 18	п. 2 ст. 29: нарушения компьютерных данных	ст. 8
Неправомерное воздействие на данные	ст. 4	Информационная преступность	ст. 8	п. 2 ст. 29: нарушения компьютерных данных	ст. 9
Неправомерное воздействие на функционирование систем / ИТ	ст. 5: компьютерных систем	Информационная преступность	ст. 6: ИТ	п. 1 ст. 29: атаки на компьютерные системы	ст. 10: ИКС
Противозаконное (неправомерное) использование	ст. 6: устройств	Информационная преступность	ст. 9: ИТ средств	—	ст. 11: устройств

[634] С учётом различия подходов ряда государств проект, внесённый Российской Федерацией в 2021 г., промежуточные версии и финальный текст значительно разнятся. Учитывается только конечный вариант, поскольку именно он предложен для подписания государствам.

устройств / ИТ средств					
Подлог	ст. 7: с использованием компьютерных технологий	Информационная преступность	ст. ст. 8, 10: данных либо с использованием ИТ средств	п. 1 ст. 29: атаки на компьютерные системы	ст. 12: с использованием ИКС
Хищение или мошенничество	ст. 8: мошенничество с использованием компьютерных технологий	Информационная преступность	ст. 11: мошенничество с использованием ИТ средств	п. 1 ст. 30: имущественные преступления	ст. 13: хищение или мошенничество с использованием ИКС
Неправомерное использование электронных платёжных средств	—	—	ст. 18	—	—
Правонарушения, связанные с авторскими и смежными правами	ст. 10	Информационная преступность	ст. 17	—	—
Правонарушения, связанные с расизмом и ксенофобией и совершаемые посредством компьютерных систем	ст. ст. 3, 4, 5 Дополнительного протокола	распространение информации, наносящей вред общественно-политической и социально-экономической системам,	—	п. 3 ст. 29: связанные с контентом	—

		духовной, нравственной и культурной среде других государств			
Отрицание или оправдание геноцида и других преступлений против человечества (человечности), совершенные посредством компьютерных систем	ст. 6 Дополнительного протокола	—	—	п. 3 ст. 29: связанные с контентом	—
Правонарушения, связанные с детской порнографией, и иные сексуальные преступления	ст. 9: через компьютерную систему	Информационная преступность	ст. 12: через ИТ	п. 3 ст. 29: связанные с контентом	ст. 14: преступления, связанные с размещением в интернете материалов со сценами сексуальных надругательств над детьми или их сексуальной эксплуатации ст. 15: домогательство или создание доверительных отношений с целью совершения

					сексуального преступления в отношении ребенка ст. 16: распространение интимных изображений без согласия
Правонарушения террористического характера	—	Информационный терроризм	ст. 15: совершенные посредством ИТ	—	—
Отмывание доходов, полученных преступным путём	—	—	ст. 15: совершенные посредством ИТ	—	ст. 17
Правонарушения, связанные с незаконным оборотом	—	Информационная преступность	ст. 16: связанные с организованной преступностью и совершенные посредством ИТ	—	—
Правонарушения против публичного порядка, морали и безопасности	—	распространение информации, наносящей вред общественно-политической и	ст. 12, 13, 14, 15	п. 3 ст. 29: связанные с контентом	—

		социально-экономической системам, духовной, нравственной и культурной среде других государств			
Правонарушения, связанные с проведением расследования правоохранительными органами	п. 3 ст. 16, п. 3 ст. 20, п. 3 ст. 21	—	п. 3 ст. 23, п. 3 ст. 28, п. 3 ст. 29	п. 4 ст. 29: преступления, связанные с мерами безопасности электронных сообщений	—
Отягчающие обстоятельства за конвенционное преступление, совершенное с использованием ИТ средств	—	—	ст. 21	+	—
Информационная война	—	+	—	—	—
Использование доминирующего положения в информационном	—	+	—	—	—

пространстве в ущерб интересам и безопасности других стран					

Таблица составлена автором

Приложение № 5. Стратегии кибербезопасности на региональном и национальном уровнях

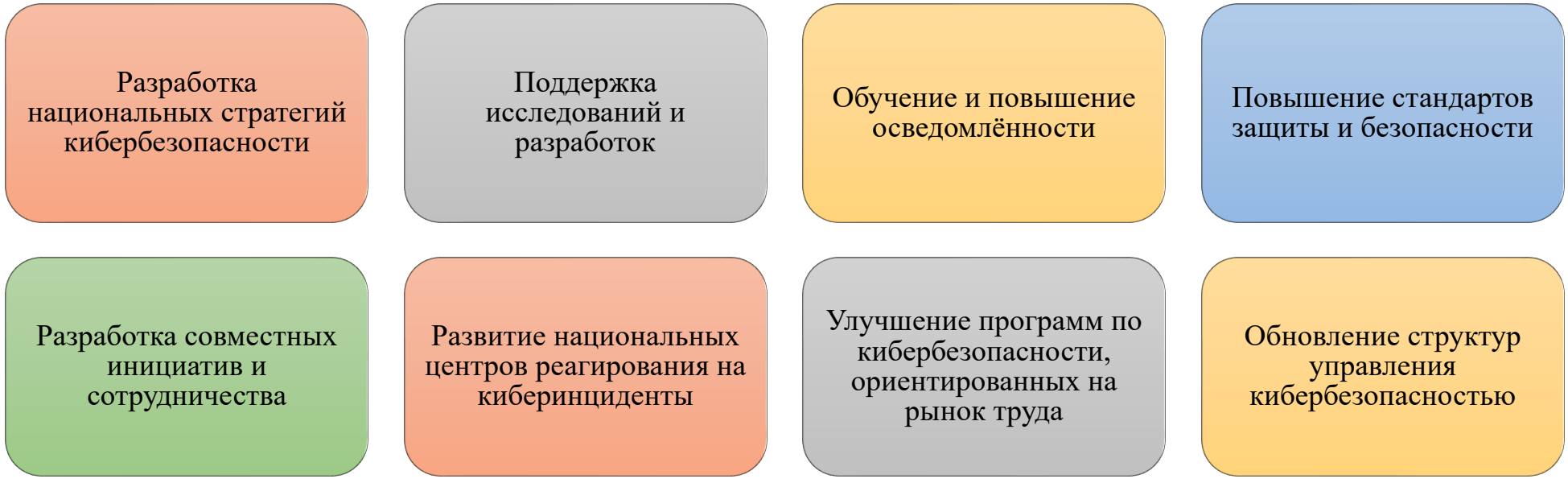
Региональный уровень

Цифровые амбиции АСЕАН



Составлено автором

Арабская стратегия кибербезопасности 2023–2027 гг. (Лига арабских государств)

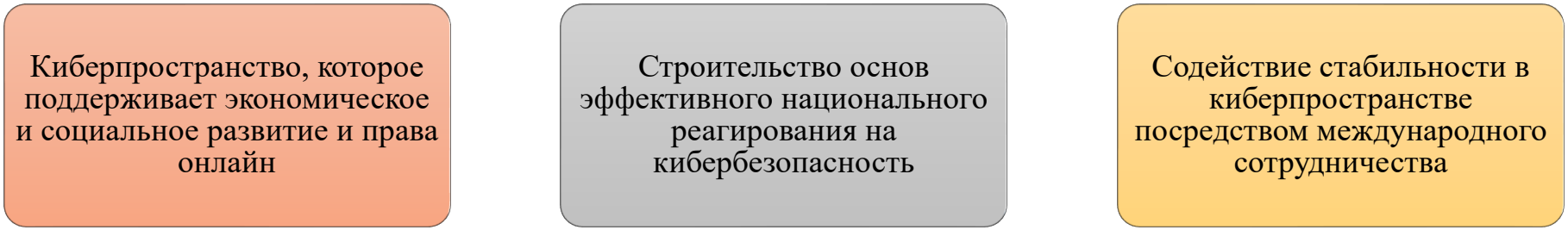


Составлено автором

Составлено автором



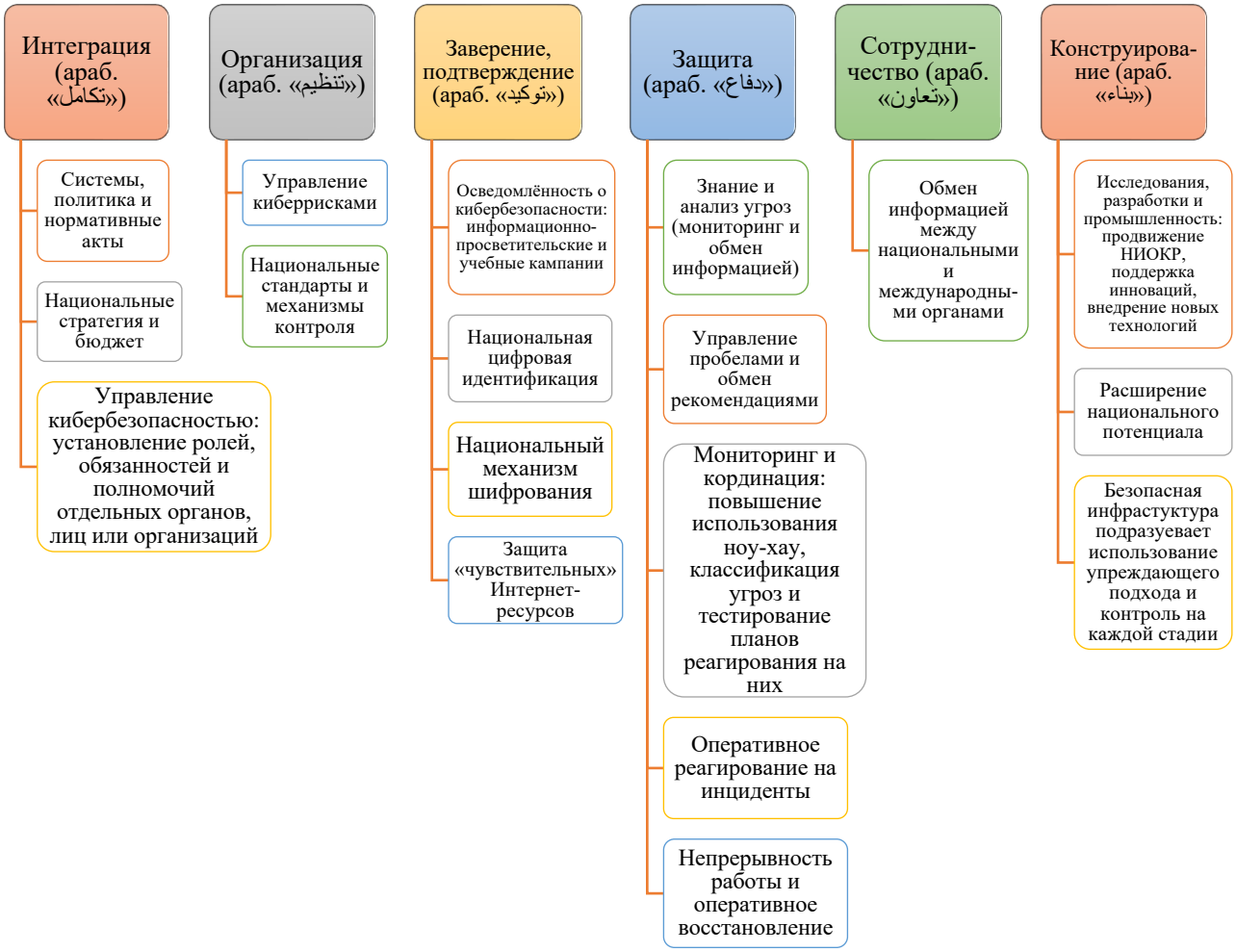
Кибердекларация Содружества Наций 2018 г.



Составлено автором

Национальные стратегии кибербезопасности

Королевство Саудовская Аравия (2020 г.)



Составлено автором

Объединённые Арабские Эмираты (2019 г.)



Составлено автором

Эмират Дубай (2017 г.)



Составлено автором

Королевство Бахрейн



Составлено автором

Государство Кувейт (2017–2020 гг.)



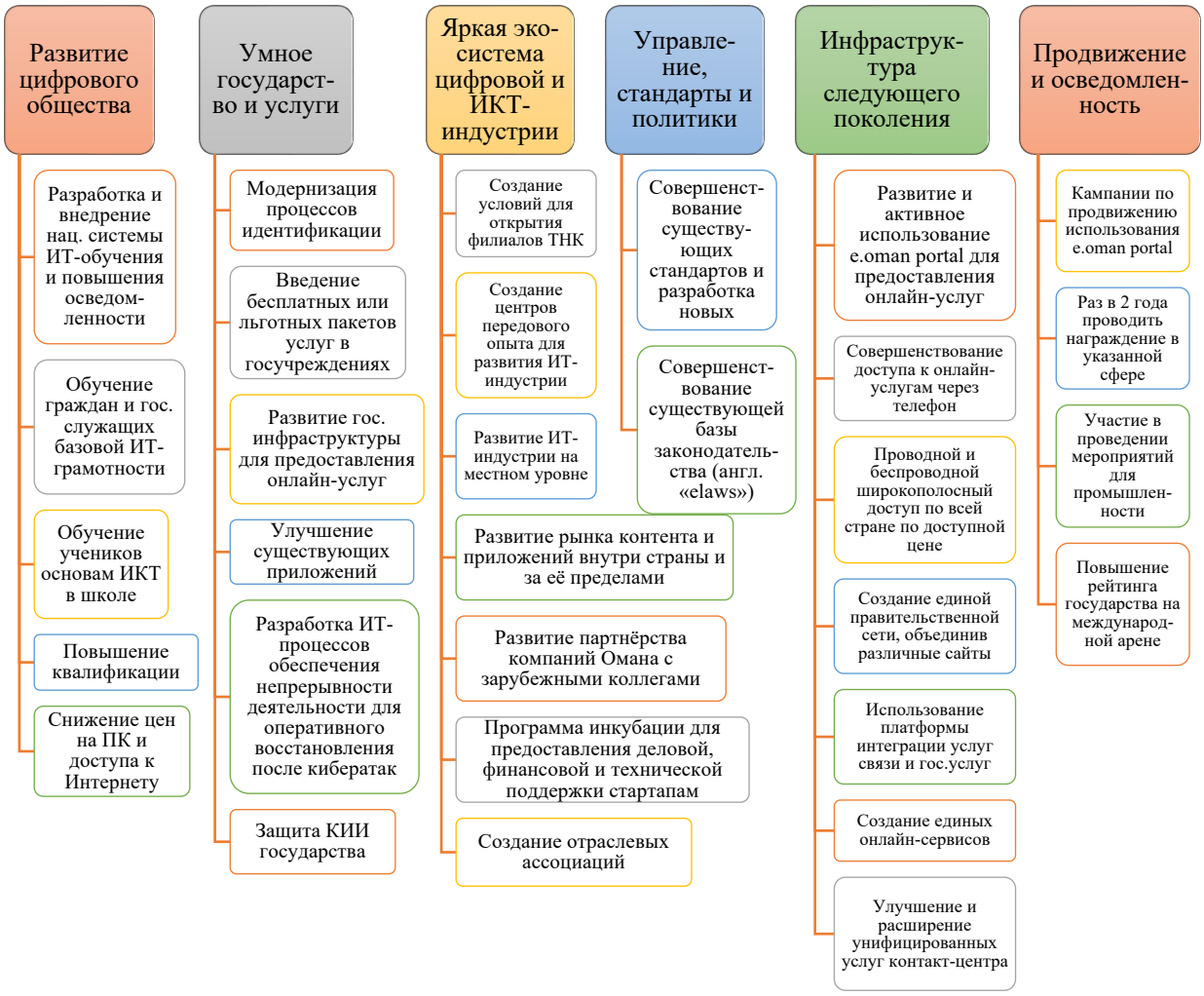
Составлено автором

Иорданское Хашимитское Королевство (2018–2023 гг.)



Составлено автором

Султанат Оман (2003/2010 гг.)



Составлено автором

Государство Катар (2024-2030 гг.)



Составлено автором



Королевство Марокко 2030 г.

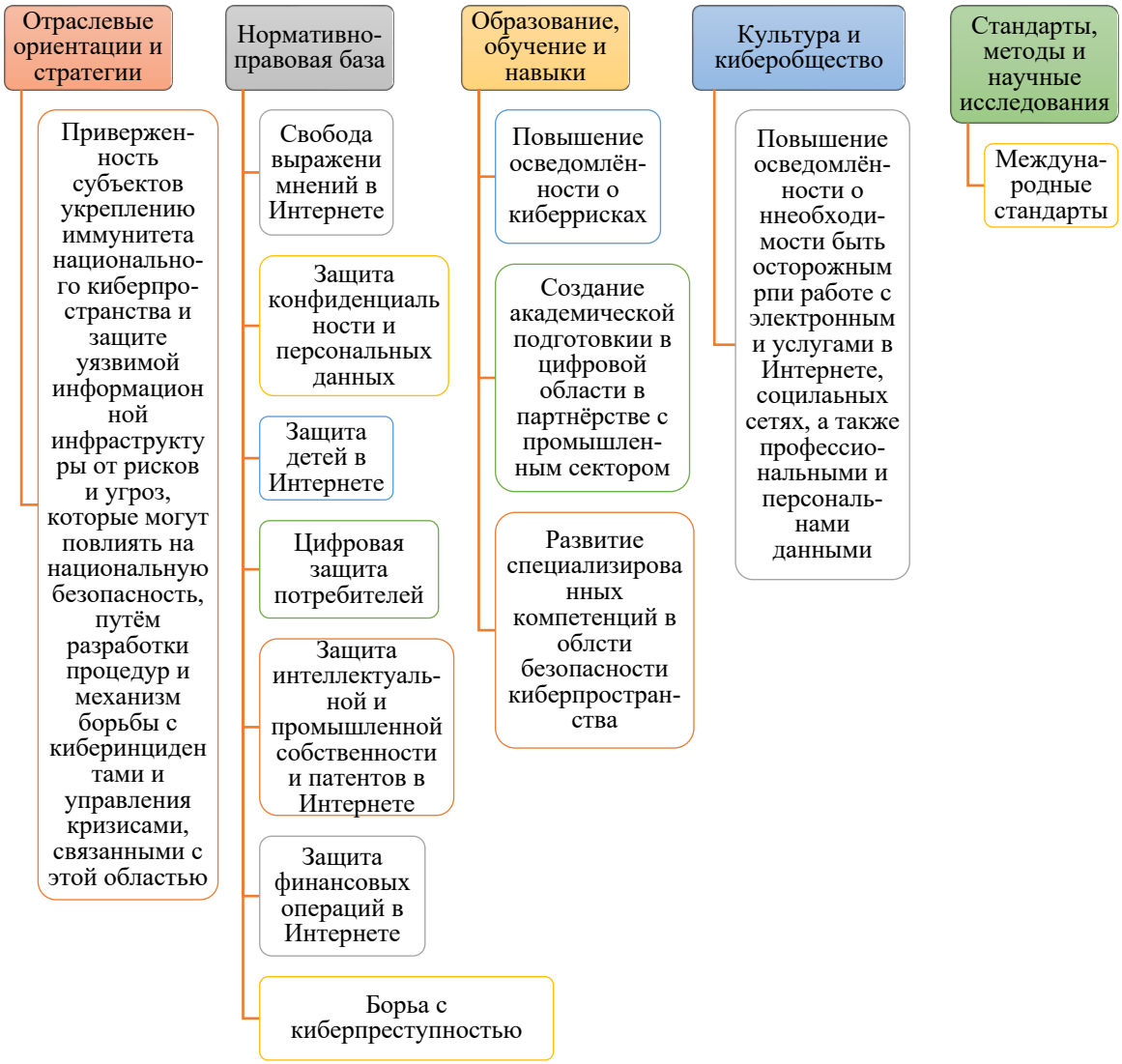
Составлено автором



Арабская Республика Египет
2023–2027 г.

Составлено автором

Тунисская Республика (2020–2025 гг.)



Составлено автором

Исламская Республика Иран 2020 г.



Составлено автором



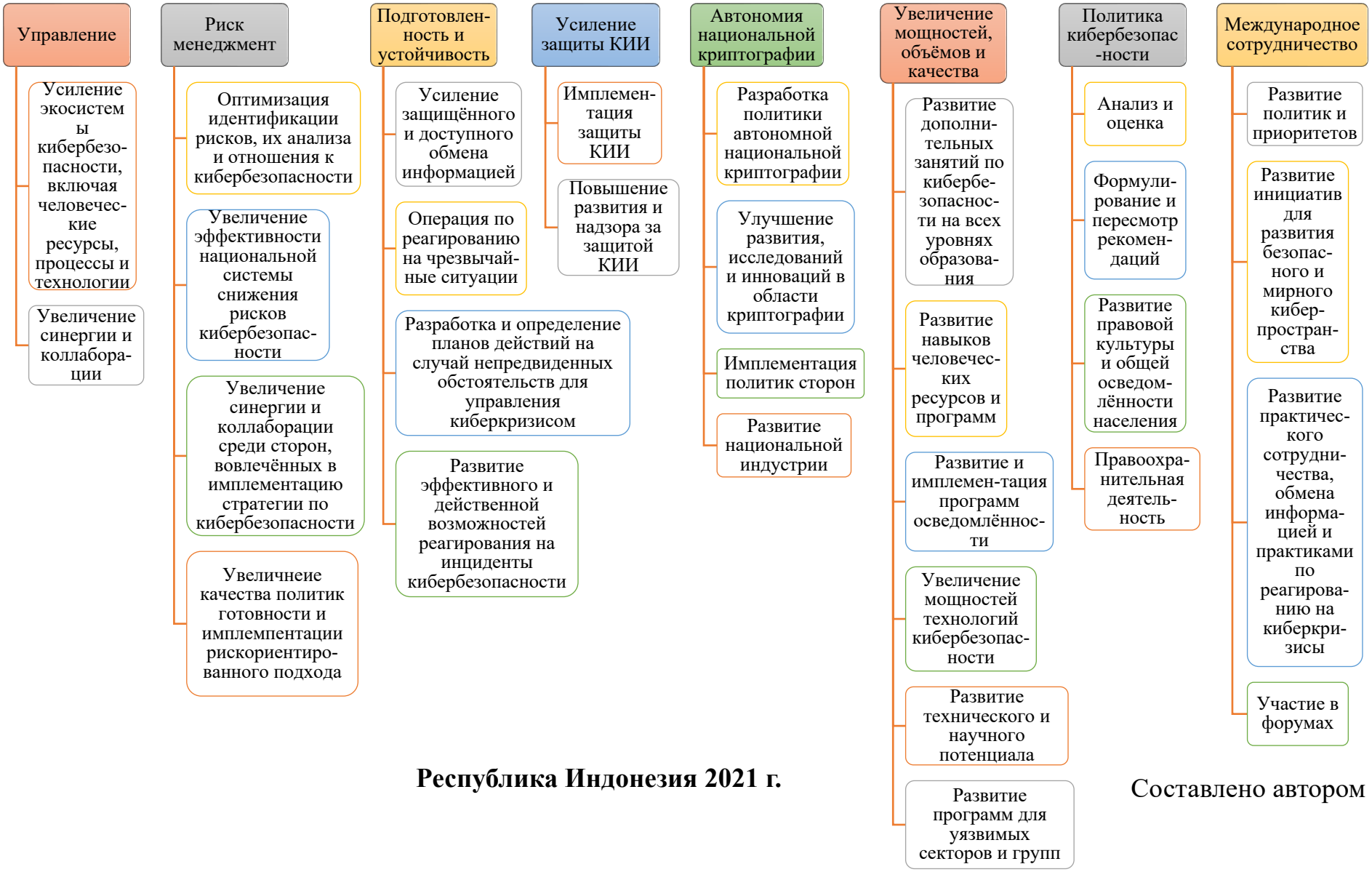
Федеративная Демократическая Республика Эфиопия 2021 г.

Составлено автором

Республика Индия (2020 г.)



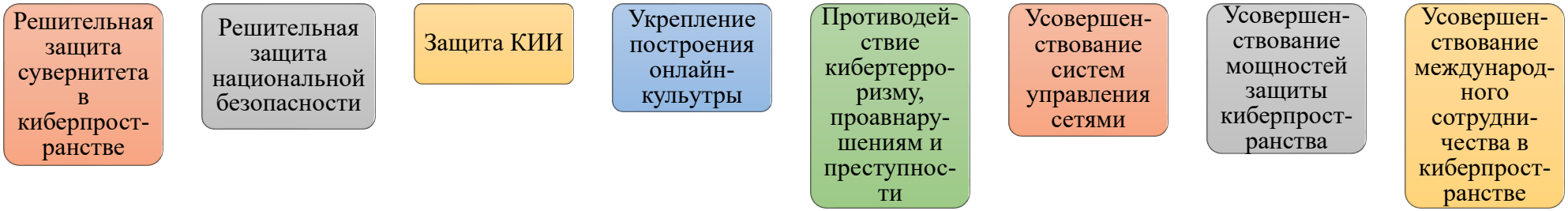
Составлено автором



Республика Индонезия 2021 г.

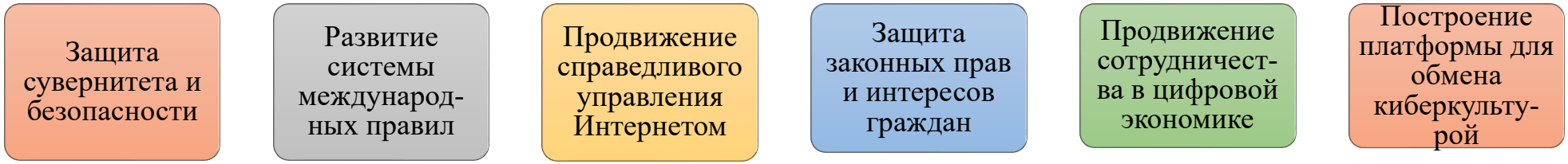
Составлено автором

Китайская Народная Республика 2016 г.



Составлено автором

Китайская Народная Республика (международное сотрудничество) 2017 г.



Составлено автором

Приложение № 6. Сферы, охватываемые стандартизацией компетентными органами государств-членов ССАГПЗ

Направления	Тематика
Безопасность корпоративной информации	Безопасность корпоративной информации
	Обязанности по безопасности корпоративной информации
Управление информационной безопасностью	Защита от вредоносного кода
	Управление информационными активами
	Мониторинг информационной безопасности
	Управление рисками информационной безопасности
	Управление инцидентами
	Управление политиками
	Физическая безопасность и безопасность среды
	Осведомлённость
	Кадры
	Управление доступом
Управление отдельных аспектов информационной безопасности	Приобретение и развитие информационных систем
	Управление изменениями
	Резервная копия и восстановление
	Электронные сервисы
Комплаенс (англ. «compliance»)	Юридические требования
	Принятые политики и процедуры
	Оценка информационной безопасности
	Аудит информационной безопасности
Внешние стороны	Клиентура
	Управление доставкой третьим лицам
	Поставщик услуг аутсорсинга (англ. outsourcing)
Иные	Управление функционированием предприятия
	Электронные СМИ
	Безопасность документации
	Конфиденциальность
	Допустимое использование
	Мошенничество и осведомители

Составлено автором на основании правового регулирования ССАГПЗ

Приложение № 7. Структура единообразной формы измерения зрелости кибербезопасности (КСА)

№	Ключевые столпы	№	Компоненты
1	Управление кибербезопасностью	**1**	Стратегия кибербезопасности
		2	Управление кибербезопасностью
		3	Политики и процедуры кибербезопасности
		4	Роли и обязанности в сфере кибербезопасности
		5	Управление рисками кибербезопасности
		6	Соблюдение законодательства, правил и стандартов в сфере кибербезопасности
		7	Периодический аудит и обзор кибербезопасности
		8	Кибербезопасность человеческих ресурсов
		9	Программы повышения осведомленности и обучения в области кибербезопасности
		10	Архитектура кибербезопасности
2	Защита кибербезопасности	**1**	Управление активами
		2	Управление учетными заверениями и разрешениями
		3	Управление сетевой безопасностью
		4	Защита мобильных устройств
		5	Защита данных и информации

		6	Шифрование и управление ключами
		7	Управление данными резервного копирования
		8	Управление уязвимостями
		9	Испытания на проникновение в сеть, компьютер, или киберпространство
		10	Управление отчетами об инцидентах и мониторинг кибербезопасности
		11	Управление угрозами кибербезопасности
		12	Финансовая безопасность
		13	Защита приложений
		14	Настройки и управление изменениями
		15	Удаленная работа
		16	Безопасность носителей
3	Устойчивость к кибербезопасности	**1**	Устойчивость кибербезопасности в управлении предприятием/органом
4	Кибербезопасность третьих лиц	**2**	Сторонняя кибербезопасность

Составлено автором на основании правового регулирования КСА

Приложение № 8. Сравнение аутентичных наименований электронных доказательств с авторским переводом на русский язык

№	Язык	Наименование доказательства на государственном языке (аутентичный текст)	Наименование доказательства на английском языке (официальный текст)	Наименование доказательства на русском языке (авторский перевод с государственного языка)
1.1	**Арабский язык**	دليل رقمي	Digital evidence	Цифровое доказательство
1.2		الدليل الإلكتروني	Electronic evidence	Электронное доказательство
1.3		الإثبات الإلكتروني		
2.1	**Персидский язык (фарси)**	ادله الکترونیکی	Electronic evidence	Электронное доказательство
2.2		ادله رایانه ای	Computer evidence	Компьютерное доказательство
3.1	**Амхарский язык**	ኤሌክትሮኒክ ማስረጃዎች	Electronic evidence	Электронное доказательство
3.2		ዲጂታል ማስረጃዎች	Digital evidence	Цифровое доказательство
4.1	**Китайский язык (традиционный)**	电子 数据	Electronic data	Электронные данные
4.2		视听 资料	Audiovisual materials	Аудиовизуальные материалы

5.1	**Индонезийский язык**	bukti elektronik	Electronic evidence	Электронное доказательство
6.1	**Французский язык**[635]	preuve électronique	Electronic evidence	Электронное доказательство

Составлено автором

[635] Несмотря на то, что официальным языком Туниса, Марокко и АНДР является арабский, законодательство также публикуется и на французском языке.