Article УДК: 341

ПРОТИВОДЕЙСТВИЕ КИБЕРПРЕСТУПЛЕНИЯМ В ОТДЕЛЬНЫХ СТРАНАХ ГЛОБАЛЬНОГО ЮГА: СОВРЕМЕННОЕ СОСТОЯНИЕ, ПРОБЛЕМЫ И ПЕРСПЕКТИВЫ

Алёна Цыплакова*

DOI 10.24833/2073-8420-2025-3-76-62-75

Введение. *В настоящем исследовании представлено краткое освещение современного состояния противодействия киберпреступлениях в странах Глобального Юга с упором на существующие преимущества, проблемы и перспективы развития внутригосударственного состояния и межгосударственного взаимодействия. Автором раскрыта используемая терминология и проведено сравнение с национальным подходом.*

Материалы и методы. *Методологически исследование строится на методах формальной логики, системном методе, а также специально-юридических методах: толковании, формально-юридическом, историко-правовом методах, а также методах юрислингвистики и лингвоюристики в части языковых особенностей использования терминов правоприменителями, законодателями и исследователями на иностранных языках. Исследование носит сравнительный характер не только в отношении непосредственно киберзаконов, но и смежного регулирования, в том числе подзаконных актов и руководящих документов. В качестве lex specialis применимо гражданское и гражданско-процессуальное право.*

Результаты исследования. *Страны Глобального Юга занимают лидирующие позиции по кибербезопасности в части законодательства, технических, организационных мер и развития потенциала, а также искусственного интеллекта, порой опережая региональный уровень по противодействию киберпреступлений. С учётом развития правового регулирования киберпосягательства охватывает широкий круг сфер, где применяются информационно-коммуникационные технологии. Под киберпреступлениями следует понимать использование высоких технологий в преступных целях, а противодействие стран Глобального Юга сфокусировано на криминализации и пенализации, профилактических мерах, экономико-технических и пресекательных инициативах, использовании технологических достижений при выявлении и расследовании посягательств, а также мониторинге и фильтрации незаконного контента.*

*** Цыплакова Алёна Дмитриевна**, преподаватель кафедры уголовного права, уголовного процесса и криминалистики МГИМО МИД России, Москва, Россия
e-mail: tsyplakova.a.d@my.mgimo.ru
ORCID ID: 0000-0001-8564-0696

Обсуждение и заключение. *В качестве проблем можно выделить отсутствие механизмов по обзору имплементации региональных конвенций именно по киберпреступлениям, различия в хранимых провайдерами услуг и владельцами платформ данных и сроках их хранения, в понимании запрещённого контента и обилие оценочных категорий, что может быть устранено посредством разработки дополнительного протокола к Конвенции ООН против киберпреступности и совершенствования национального регулирования. Отсутствие единого понимания киберпосягательств может быть нивелировано посредством ратификации упомянутого международного договора странами Глобального Юга. В странах-лидерах в области кибербезопасности реализованы технические и организационные инициативы, представляющие интерес для имплементации в отечественной практике.*

Введение

Существующий цифровой разрыв, ограниченность человеческих ресурсов и технических возможностей и явно противоположные позиции законодателей, обнаруженные при разработке Конвенции ООН против киберпреступности[1], переопределяют актуальность изучения киберрегулирования с целью совершенствования национальной нормативно-правовой базы и международных документов, а также выработки универсальных эффективных мер.

Хотя категорирование по различным индексам является динамичным, отметим прогресс среди стран Арабского Востока, Африки и Азии. Оценивая по 5 параметрам: правовые, технические, организационные меры, сотрудничество и развитие потенциала, Международный союз электросвязи о кибербезопасности в 2024 г. отнёс к образцовым и продвинутым государствам в сфере обеспечения кибербезопасности многие страны Глобального Юга[2] (в частности Королевство Бахрейн, Арабская Республика Египет, Республика Индия, Султанат Оман, Государство Катар, Королевство Саудовская Аравия, Объединённые Арабские Эмираты, Королевство Марокко, Иорданское Хашимитское Королевство, Республика Индонезия, Турецкая Республика, Малайзия, Федеративная Демократическая Республика Эфиопия и Китайская Народная Республика)[3]. Некоторые из них, в том числе КНР, ОАЭ, КСА, Малайзия, Турция и Индонезия, занимают также лидирующие позиции в Международном индексе по оценке управления искусственным интеллектом 2025 г.[4].

Вместе с тем исследования по уголовно-правовой кибертематике чаще направлены на изучение лишь одного региона либо стран так называемого Глобального Севера.

Исследование

Терминологические особенности как постановка проблематики: объём деятельности

Киберзаконы стран Глобального Юга можно поделить на три категории, содержащие указание на: ответную реакцию (арабские страны, Нигерия), непосредственно посягательства (Иран, ФДРЭ) либо же вид безопасности (Малайзия).

---

[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] Несмотря на необходимость чёткого релевантного для юридической науки понятия, в настоящее время в зависимости от социокультурного контекста, правовой культуры и традиций и целей исследования понятие «страны Глобального Юга» может видоизменяться.

[3] 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).

[4] 2025 'AI Governance InternationaL Evaluation Index (AGILE Index)' Report // Agile Index. URL: https://agile-index.ai (дата обращения: 04.08.2025).

Учитывая лингвистическое разнообразие стран Глобального Юга, необходимо дать уточнения в контексте восточных языков. В *арабском* языке глагол «мана'а» (араб. «منع») может обозначать предотвращение, профилактику, запрет и предупреждение в зависимости от контекста[5]. Традиционно в юридических текстах арабских стран самым распространенным термином является борьба — «*мукяяфахатун*» (араб. «مكافحة»). В нормативно-правовых актах встречаются также термины «*мувааджагатун*» (с араб. «مواجهة» буквально противостояние или встреча лицом к лицу) и «*викаяатун*» (с араб. «وقاية» — предупреждение, предохранение, профилактика, поскольку образован от глагола «وقى» — охранять, защищать). Сопоставляя содержание нормативно-правовых актов, отметим, что перечисленные термины как деятельность охватывают зачастую криминализацию и пенализацию посягательств, уголовно-процессуальные аспекты (доказывание, следственные действия, особенности наложения ограничительных мер), особенности установления уголовной юрисдикции, назначение компетентного органа с указанием полномочий и международное сотрудничество.

В *турецком* законодательстве используется в основном два термина: тур. «*mücadele*» и тур. «*önleme*» — закон Турецкой Республики № 3713 от 12.04.1991 «О борьбе с терроризмом» (тур. Terörle Mücadele Kanunu) и закон Турецкой Республики № 5549 от 18.10.2006 «О предотвращении отмывания доходов от преступности» (тур. Suç Gelirlerinin Aklanmasinin Önlenmesi Hakkinda Kanun). При этом «*mücadele*» происходит от арабского масдара «*муджаадалятун*» («مجادلة» — спор)[6]. По содержанию они охватывают, помимо перечисленного выше, контроль, мониторинг, исполнение приговоров, административную ответственность, защитные меры для информаторов.

Сходная ситуация и с персидским термином «*мобарэзэ*» (пер. «مبارزه»), который заимствован из *арабского* языка — «*мубаараза-тун*» (араб. «مبارزة» — дуэль). Он распространен в военной сфере, однако в юриспруденции используется как «борьба» или «предупреждение»: Закон Исламской Республики Иран от 22.01.2008 «О борьбе с отмыванием денег» (перс. «قانون مبارزه با پولشویی») и Закон Исламской Республики от 12.03.2016 «О борьбе с финансированием терроризма» (перс. «قانون مبارزه با تأمین مالی تروریسم»). При этом в юридической литературе [4,6,7,8,9,12] превенция чаще всего обозначается термином «*пишгир*» (пер. «پیشگیری»), который означает профилактику вне правового контекста . При этом именно в киберзаконе (Закон ИРИ от 25.05.2009 «О компьютерных преступлениях») вообще отсутствует указание на форму деятельности, при этом детализирует уголовную ответственность юридических лиц, обязанности поставщиков услуг и содержание необходимых подзаконных актов.

В отечественной же юридической мысли наиболее широким термином является именно противодействие, охватывая борьбу, профилактику и минимизацию (устранение) последствий. Признание деяния преступным и наказуемым остаётся за рамками в данном случае, поскольку единственным источником уголовного законодательства является исключительно Уголовный кодекс в отличие от зарубежных стран, где отмечается множественность правовых регуляторов.

Кибер-составляющая как центральная проблема

С учётом генезиса норм, криминализующих и пенализующих так называемые киберпреступления 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 всевозможных информационных технологий в преступных целях (широкий подход во второй половине 2010-х и 2020-х годах).

Даже в рамках одного региона (арабского, азиатского или африканского) нет единой позиции ни при определении, ни при наполнении содержания рассматриваемых посягательств. Преступления в сфере информационных технологий стали охватывать деяния, связанные с запрещённым

[5] تعريف و معنى منع في معجم المعاني الجامع - معجم عربي عربي // Al-maany. URL: https://www.almaany.com/ar/dict/ar-ar/منع/ (дата обращения: 19.05.2025).

[6] Mücadele // Sevan Nişanyan. URL: https://www.nisanyansozluk.com/kelime/mücadele (дата обращения: 19.07.2025).

[7] پیشگیری // Abadis. URL: https://abadis.ir/fatofa/پیشگیری/ (дата обращения: 18.07.2025).

содержанием информации в сети «Интернет» (дезинформация, слухи, фэйковые новости, порнографические материалы, клевета, жестокое обращение с детьми, радикализм / сепаратизм, нарушение правил пользования социальными сетями и мессенджерами), экономические посягательства (кража, мошенничество, подлоги, нарушения прав интеллектуальной собственности и интересов потребителей, азартные игры, правонарушения в сфере электронной торговли, онлайн-банкинга), непосредственно компьютерные преступления (кибератаки, неправомерный доступ и нарушение целостности, конфиденциальности и доступности), нарушения лицензионных видов деятельности (оказание сертифицированных и телекоммуникационных услуг, искусственного интеллекта, разработки программного обеспечения, Интернет-кафе, онлайн-игры), деяния против государственной власти (правонарушения в сфере электронного документооборота, систем уведомлений, оказания государственных услуг, электронного голосования, цифровой трансформации и подлог цифровых доказательств). Перечисленные сферы являются одновременно и конституирующим признаком — зачастую предметом (целью) либо средством (источником) посягательства.

Несмотря на терминологическое многообразие на иностранных языках, в официальных переводах используется понятие именно *киберпреступления*. Как указывается в Федеральном декрете-законе ОАЭ № 34 от 20.09.2021 «О борьбе со слухами и электронными преступлениями», «*ас-сибраани*» (араб. «السبراني») или «*кибер*» подразумевает «*всё, что связано с компьютерными информационными сетями, Интернетом, различными информационными программами и всеми услугами, которые предоставляются в рамках перечисленного*», охватывая виртуальное взаимодействие и оборудование, то есть весь аппаратно-программный комплекс.

Хотя киберпреступления ассоциируются с англоязычной калькой, приставка *кибер* должна восприниматься как отсылка к разделу физики — кибернетике — науке о закономерностях получения, хранения, обработки и передачи информации в системах, то есть взаимодействии информационной среды с субъектами и управлении ею. Компьютер как основная единица инфраструктуры является либо обязательным элементом (с англ. «cyber-dependent crimes» — буквально *кибер*зависимые преступления), либо расширяет преступный потенциал (с англ. «cyber-enabled crimes» — буквально преступления с *кибер*возможностями).

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[8], предусмотренные наказания свидетельствуют о возможности вменения как административного правонарушения[9], так и уголовно наказуемого деяния (араб. «الأفعال المجرمة»). То же самое касается регулирования отдельных видов лицензирования (телекоммуникаций и СМИ[10]) и защиты персональных данных. (Письменное) предупреждение, отзыв лицензии, *административный* штраф[11], временное приостановление и/или прекращение доступа к электронной системе[12], временное приостановление деятельности, отказ от услуг (индонез. «pencabutan layanan») и принудительные полицейские меры (индонез. «daya paksa

[8] 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// Комитет по законодательным и правовым вопросам Маджлис Аш-Шура Королевства Бахрейн. URL: https://inlnk.ru/20RAJN (дата обращения: 25.03.2025).

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

[10] 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».

[11] Характерно для всех изучаемых стран Глобального Юга.

[12] 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 // Законодательная база Республики Индонезия. URL: https://peraturan.bpk.go.id/details/274494/uu-no-1-tahun-2024 (дата обращения: 04.05.2025).

polisional»)[13] с возможной публикацией правонарушения на веб-сайте министерства по решению Министра юстиции и прав человека Республики Индонезия[14] налагаются уполномоченными органами в соответствующей сфере (в арабских странах, например, Управлением по искусственному интеллекту Королевства Бахрейн, Комиссией КСА по информационно-коммуникационным технологиям, Министром транспорта, связи и информационных технологий Султаната Оман), 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.

Наименование и содержание деяний имеют особое значение для соблюдение принципа двойной криминальности и установления уголовной юрисдикции государства в виртуальном пространстве при осуществлении международного сотрудничества в сфере уголовного судопроизводства, без которого не обойтись при уголовном преследовании за рассматриваемый вид преступлений ввиду трансграничного характера и вовлеченности нескольких (а порой и множества) иностранных государств.

Необходимо также учитывать, подписантами каких международных договоров являются отдельные страны Глобального Юга и какова степень имплементации разнящихся документов. В отдельных случаях национальное регулирование служило основой для международных документов: Положение Королевства Саудовская Аравия от 27.03.2007 «О борьбе с преступлениями в сфере информатики» легло в основу Арабской конвенции, при этом она до сих пор не ратифицирована Королевством[15]; в иных случаях — наоборот: на страны аль-Магриба оказала влияние Будапештская конвенция. Королевство Марокко подписало её 29.06.2018 и ратифицировало 01.10.2018 для восполнения пробелов[16], Тунисская Республика — 08.03.2024 и 01.07.2024, соответственно, а Нигерия — 06.07.2022 и 01.11.2022.

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).

Современное состояние: сопоставление национальных и региональных подходов

В специализированной литературе, международных документах, нормативных правовых актах различных органов государственной власти Российской Федерации и стран Глобального Юга встречается многообразие понятий, которые используются для описания ответной реакции личности, общества и государства на преступность. При характеристике деятельности необходимо определить круг субъектов воздействия, направления и уровни взаимодействия, охраняемые интересы, понятийный аппарат и страновой охват.

Сопоставление межгосударственного и внутригосударственного уровней позволяет выявить следующие особенности. 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[17]) или отставая от национального уровня (арабский и африканский регионы). Наглядным примером первого является АСЕАН: борьба именно с киберпреступностью ведётся в первую очередь в рамках программ по предупреждению

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

[14] Ст. ст. 225, 228 решения Министра коммуникаций и информатики Республики Индонезия № 5 от 01.04.2021 «О внедрении телекоммуникаций».

[15] التصديق على الاتفاقيه العربية لمكافحة جرائم تقنية المعلومات // Лига арабских государств. URL: http://www.leagueofarabstates.net/ar/legalnetwork/Documents/%العربية%20الاتفاقيه%20على%20التصديق%20المعلومات%20تقنية%20جرائم%20لمكافحة20.pdf (дата обращения: 09.03.2025).

[16] 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.

[17] Наглядным примером может служить АСЕАН.

транснациональной преступности, о чём было принято решение во время 3-ей Встречи АММТС (Сингапур, 11.10.2001): в План действий по борьбе с транснациональной преступностью (Янгон, 23.06.1999) были внесены соответствующие изменения[18]. 14.01.2011 был принят первый Генеральный план АСЕАН в сфере ИКТ, который дважды обновлялся впоследствии (в 2015 и 2025 гг.).

Рисунок № 1. Цифровые амбиции АСЕАН (переведено и составлено автором)[19]

В то время как национальные стратегии кибербезопасности арабских датируются 2010-ми гг., руководящие документы регионов — 2020 гг. (см. пример — Рисунок № 2).

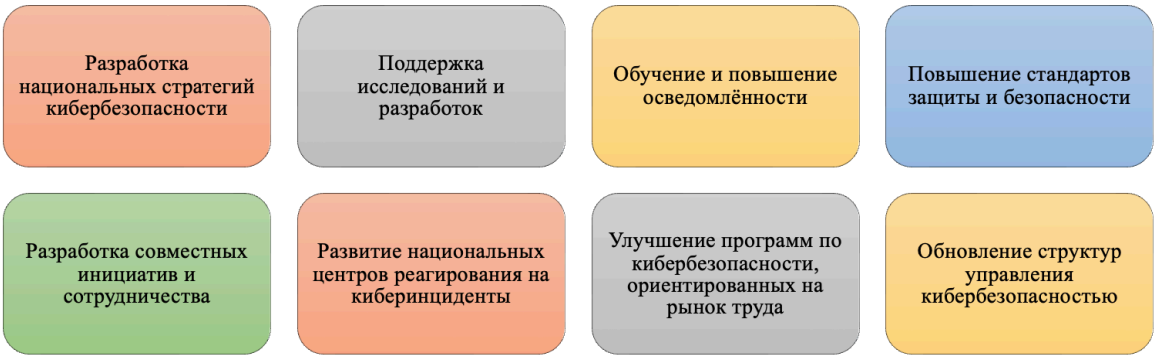

Рисунок № 2. Арабская стратегия кибербезопасности 2023–2027 гг. (Лига арабских государств) (переведено и составлено автором)[20]

[18] 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).

[19] 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).

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

Вдобавок создаются универсальные институциональные механизмы по типу министерских встреч, рабочих групп, исполнительных комитетов по кибертематике (цифровой трансформации, электронным торговле и правительству, использованию ИКТ)[21], противодействию организованной преступности, а также общеуголовной направленности: полицейские службы и конференции по исполнению конвенций. Последнее характерно как для универсального, так и регионального уровней, хотя пока и не касается именно киберпреступлений: Конференции по исполнению международных договоров учреждены в рамках ООН (e.g., в отношении Палермской[22] и Меридской[23] конвенций), Организации исламского сотрудничества[24], Организации американских государств[25], однако таковых механизмов нет в отношении Соглашения Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности (Екатеринбург, 16.06.2009)[26], Конвенции Африканского союза против кибербезопасности и защиты персональных данных (Аддис-Абеба, 27.06.2014)[27], Арабской Конвенции о борьбе с преступлениями в области информационных технологий (Каир, 21.12.2010)[28] за исключением Конвенции против киберпреступности (Будапешт, 23.11.2001)[29] и Конвенции ООН против киберпреступности.

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 [10]. 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 (см. примеры — Рисунки №№ 3, 4).

---

[21] Характерно для АСЕАН, БРИКС, Совета сотрудничества арабских государств Персидского (Арабского) залива и Лиги арабских государств.

[22] Генеральная Ассамблея ООН: Резолюция 55/25, принятая Генеральной Ассамблеей 15 ноября 2000 года «Конвенция Организации Объединенных Наций против транснациональной организованной преступности» // Документ ООН A/RES/55/25, 15 November 2000.

[23] Генеральная Ассамблея ООН: Резолюция 58/4, принятая Генеральной Ассамблеей 31 октября 2003 года «Конвенция Организации Объединенных Наций против коррупции» // Документ ООН A/RES/58/4, 31 October 2003.

[24] OIC/CLE-1/2023/MIN/FINALCONVENTION//OIC.URL:https://www.oic-oci.org/docdown/?docID=9771&refID=4268 (accessed 20.04.2025).

[25] Механизм мониторинга осуществления Межамериканской конвенции против коррупции (исп. «MESICIC»).

[26] Соглашение между Правительствами государств-членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности (Екатеринбург, 16 июня 2009 г.).

[27] 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 (accessed 09.03.2025).

[28] الاتفاقية العربية لمكافحة جرائم تقنية المعلومات // Лига арабских государств. URL: http://www.lasportal.org/ar/legalnetwork/Documents/لمكافحة%20جرائم%20تقنية%20المعلومات%20التصديق%20على%20الاتفاقية%20العربية%20.pdf (дата обращения: 09.03.2025).

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

Рисунок № 3. Национальная стратегия кибербезопасности Арабской Республики Египет 2023–2027 гг. (переведено и составлено автором)[30]

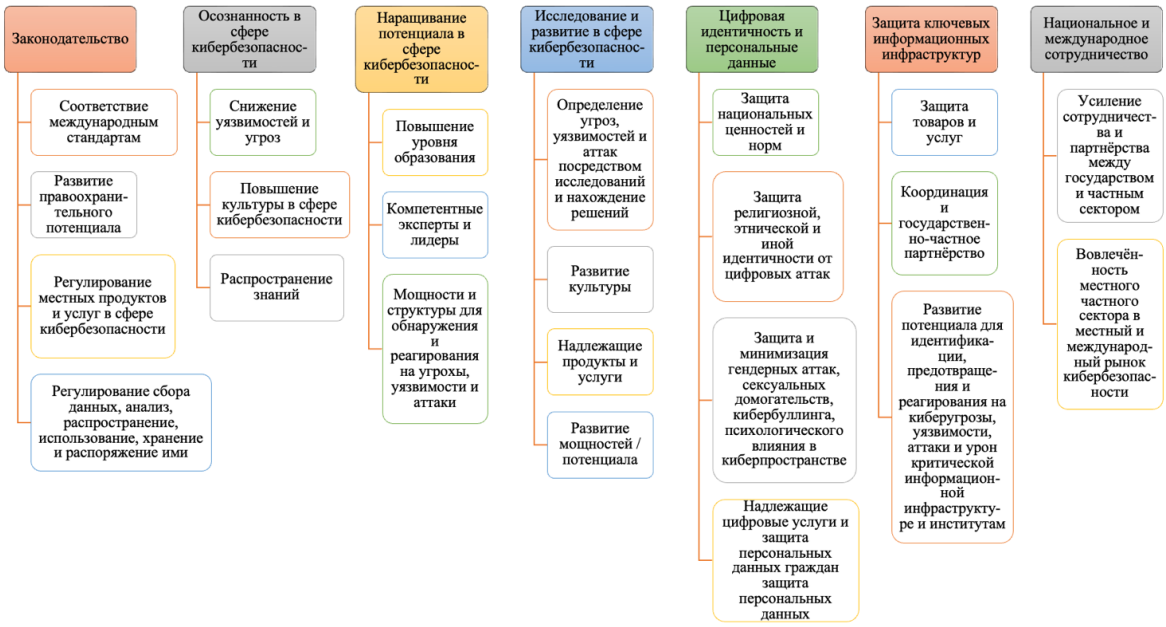

Рисунок № 4. Национальная политика и стратегия кибербезопасности Федеративной Демократической Республики Эфиопии 2021 г. (переведено и составлено автором)[31]

[30] الاستراتيجية الوطنية للأمن السيبراني ٢٠٢٣ ٢٠٢٧. // Egyptian CERT. URL: https://mcit.gov.eg/Upcont/Documents/Publications_1412024000_ar_National_Cybersecurity_Strategy_2023_2027.pdf (accessed 05.08.2025).

[31] 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).

Среди специализированных органов (в широком смысле) выделяются как непосредственно[32], так и опосредованно участвующие в уголовном судопроизводстве. 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 (ОЭЗ / СФЗ), 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, особенно в ОЭЗ (СФЗ), а также в сфере защиты персональных данных могут 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) [1].

В отдельных странах Глобального Юга (Эфиопия, арабские страны, Иран) существует тенденция привлечения обладающих специальными познаниями должностных лиц из конкретных министерств, ведомств и государственных учреждений (причём при расследовании не только киберпреступлений [2]), что целесообразно использовать и в отечественной практике.

Профилактика уязвимых групп в вопросах киберпреступлений выражается в активном вовлечении научного и гражданского сообщества на мероприятиях с архитектурой нулевого доверия, стандартизации, волонтёрстве (Республика Индия[33]) и амбассадорстве (Оман[34] и ОАЭ[35]); пресекательная деятельность — создании платформ, систем безопасности и баз данных по контролю и мониторингу контента, движению денежных средств по типу «goAML»[36] и «MuleHunter»[37], виртуальных активов, подозрительных IP-адресов[38], абонентских номеров, электронных почтовых ящиков, Интернет-ресурсов, банковских аккаунтов[39], обмену и выявлению уязвимостей[40], доступ к которым не только у правоохранителей, но и граждан[41].

Типологически одними из самых распространённых видов киберпреступлений были и остаются мошенничества, а также распространение запрещённого контента. 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). Закрытие Интернет-ресурсов, ограничение доступа к ним или информации зачастую производится

[32] Создаются уполномоченные структурные подразделения в правоохранительных органах и судах, либо же традиционным органам предоставляются особые полномочия.

[33] Cyber Crime Volunteer Program // Vijetha IAS Academy. URL: https://vijethaiasacademy.com/blog/Cyber-Crime-Volunteer-Program (accessed 11.06.2025).

[34] أهداف برنامج سفراء السلامة المعلوماتية // Национальный центр информационной безопасности Султаната Оман. URL: https://ambassadors.cert.gov.om/about_ar.aspx (дата обращения: 13.06.2025).

[35] السلامة السيبرانية والأمن الرقمي // 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).

[36] Проект ООН // УНП ООН. URL: https://www.unodc.org/unodc/en/global-it-products/goaml.html (дата обращения: 16.05.2025).

[37] 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).

[38] اللجنة الوزارية للحكومة الالكترونية بدول مجلس التعاون تعقد اجتماعها الخامس في البحرين // Исполнительный комитет электронного правительства ССАГПЗ. 21.03.2017. URL: http://www.gcc-egov.org/ar/news_details?id=758559 (дата обращения: 25.03.2025).

[39] Приложение для предотвращения кибермошенничества [11].

[40] MASSA // MyCERT. URL: https://www.mycert.org.my/portal/full?id=1559520b-fa96-4a5e-9ce8-99f39f7d3442 (accessed 06.08.2025); MISP // MyCERT. URL: https://www.mycert.org.my/portal/full?id=89df3ade-427f-4ab0-ba1f-219850d31c76 (accessed 06.08.2025).

[41] Второе касается баз данных подозрительных абонентских номеров, электронных почт, Интернет-ресурсов и IP-адресов в Индии и безопасности устройств Малайзии.

в административном порядке с возможностью обжалования в суде (в ОАЭ — прокуратура, в Республике Индия — назначенные центральным правительством должностные лица; в Индонезии — министр телекоммуникаций и информатики), однако возможно и привлечение общественности, в том числе киберволонтёров. В Азии также действуют продвинутые автоматизированные системы по фильтрации контента, разработанные правительством и научным сообществом по типу «Золотой щит»[42], основываясь на негативных комментариях, вульгарном поведении пользователей и остроте тематики [5]. В КНР выделяется негативный и запрещённый контент:

- использование преувеличенных названий или наименований, которые серьёзно не соответствуют содержанию; сенсационные сплетни, скандалы, проступки и т. д.; ненадлежащее комментарии о стихийных бедствиях, крупных авариях или других катастрофах; контент, который имеет сексуальные инсинуации, является сексуально наводящим или легко ассоциируется с сексом; контент, который вызывает физический или психологический дискомфорт; подстрекательство к дискриминации в отношении групп или регионов; пропаганда грубого, непристойного или вульгарного контента; контент, который может привести к тому, что несовершеннолетние подражают небезопасному поведению или поведению, которое нарушает социальные нормы, или вызывает вредные привычки для несовершеннолетних и т. д.;

- противоречие принципам Конституции; угроза национальной безопасности, разглашение государственной тайны, подрыв национального режима и разрушение национального единства; вред чести и интересам нации; искажение, очернение, осквернение или отрицание поступков и духа героев и мучеников; ущерб именам, изображениям, репутации и чести героев и мучеников посредством оскорбления, диффамации или других подобных средств; пропаганда терроризма или экстремизма или подстрекательство к совершению террористической или экстремистской деятельности; разжигание этнической ненависти или этнической дискриминации или подрыв этническое единство; подрыв политики страны в отношении религий или пропаганда культов и суеверий; распространение слухов, нарушающих экономический или социальный порядок, непристойности, секса, азартных игр, насилия, убийств, террора или подстрекательство к преступности; оскорбления или клевета, нарушения чести, неприкосновенности частной жизни или других законных прав и интересов третьих лиц; а также

- нарушение общественных интересов, кража личности, получение неправомерной выгоды[43].

Исходя из системного толкования и передовых практик арабских и азиатских стран (в частности ОАЭ, КСА, Марокко, 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, ненависть к племенам, религиям, расам и межгруппам, национальное единство, моральные принципы, безопасность государства, сохранение дружественных отношений.

Помимо фильтрации и мониторинга контента, на владельцев социальных платформ и поставщиков услуг возлагается обязанность по хранению сведений о пользователях и их действиях. 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

[42] В 2003 г. также было громкое обсуждение т.н. системы обзора контента Фалуньгун, разработанной Китайской академией наук, однако по заявлениям представителей Академии она нацелена на любую вредную для КНР информацию. См. "法轮功内容审查系统"开发者指中新网报导不实 // Epoch Times. 26.02.2003. URL: https://www.epochtimes.com/gb/3/2/26/n279788.htm (accessed 05.08.2025).

[43] 互联网用户账号信息管理规定 // Онлайн-законодательство КНР. URL: https://www.cac.gov.cn/2022-06/26/c_1657868775042841.htm (дата обращения: 02.05.2025), 《网络信息内容生态治理规定》全文 // Онлайн-законодательство КНР. URL: http://media.people.com.cn/n1/2019/1220/c40606-31516139.html (дата обращения: 02.05.2025).

местоположением пользователя. Срок хранения данных варьируется в среднем от полутора месяцев – полугода до двух лет: 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; Тунис — min. 2 года; Иран — не менее 15 дней трафик и не менее 6 месяцев хостинг-услуги.

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). Сотрудничество может быть как добровольным, так и по решению суда [3]. Нарушение обязанности сотрудничать может влечь наложение юридической ответственности, вплоть до уголовной[44]. При этом нет законодательно жёсткой «привязки» к привлечению специалиста (эксперта)[45]; исходя из т.н. белых книг, составленных представителями науки и правоприменителями[46], предполагается, что прокурор или полицейский должны быть технически подкованы и иметь соответствующую квалификацию или хотя бы минимальные «представления» о специфике цифровых следов.

При расследовании киберпреступлений решающую роль играют не только сведения, представляемые поставщиками услуг и владельцами платформ, но и иные электронные доказательства, которые могут быть получены в ходе обыска, выемки[47], изъятия[48], перехвата и прослушивания контента[49], контроля сообщений, наблюдения, дистанционных и физических «цифровых расследований», электронного мониторинга, извлечения и копирования данных, производимых как с судебным решением, так и без него. При этом отсутствие деления на оперативно-розыскные мероприятия и следственные действия и открытый перечень последних (e.g., в арабских странах) способствует гибкости процесса получения и фиксации доказательственной информации и дополняется расширенным перечнем лиц, привлекаемых для производства процессуальных действий. Активно обсуждаются и применяются специализированные информационные системы для уведомлений и получения судебных решений, электронного документооборота, Блокчейн для обеспечения целостности цифровых доказательств и отслеживания цепочки хранения[50], искусственного интеллекта при обработке большого массива данных[51]. Всё это должно учитываться при организации международного сотрудничества в сфере уголовного судопроизводства и возможной имплементации в отечественный уголовный процесс.

Заключение

Таким образом, киберпреступления — это использование высоких технологий в преступных целях (в широком смысле), а противодействие им в странах Глобального Юга — это комплексная деятельность правоохранительных и специализированных государственных органов, органов законодательной

[44] Для юридических лиц — скорее административные штрафы.

[45] Эксперты скорее работают с т.н. статикой, хранящейся на изъятом материальном носителе, в то время как специалисты — с «динамикой», содержащейся в Интернет-пространстве.

[46] В пример можно взять Руководство Арабского университета наук безопасности им. принца Наифа бин Абдель Азиза 2024 г., Руководство по расследованию киберпреступлений, разработанное Советом по цифровой безопасности Индии с участием правоохранительных органов, а также узкопрофильные руководства Центра по исследованию и обучению расследований киберпреступлений. См. Center For Cybercrime Investigation Training & Research // DSCI. URL: https://www.dsci.in/content/ccitr (accessed 08.04.2025), 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), [13].

[47] Выемки в КСА требуют судебного решения в отличие от ОАЭ. В АРЕ не требуется судебного решения на все перечисленные действия; в Катаре — в отдельных случаях достаточно решения Генерального прокурора; в АНДР — согласие компетентного прокурора.

[48] В ИРИ требуется судебное решение.

[49] В ФДРЭ с разрешения Министра.

[50] 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).

[51] AI for Safer Children // UNICRI. URL: https://unicri.org/topics/AI-for-Safer-Children (accessed 12.04.2025).

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 дву- и многостороннем форматах. Динамика противодействия разнится в регионах Глобального Юга: опережающими являются азиатский и арабский, а догоняющим — африканский. Инструментарий на международном уровне сосредоточен не только (и не сколько) на киберпреступности, сколь более общих вопросах безопасности, особенно на профилактических мерах. В качестве проблем отметим отсутствие механизмов по обзору имплементации региональных конвенций именно по киберпреступлениям, различия в понимании запрещённого контента и обилие оценочных категорий, различия в хранимых провайдерами услуг и владельцами платформ данных и сроках их хранения, отсутствие единого понимания киберпосягательств, которое, возможно, станет более гармонизированным при условии подписании и ратификации Конвенции ООН против киберпреступности странами Глобального Юга. Часть из проблем может быть решено посредством разработки дополнительного протокола, а также совершенствования национального регулирования. В странах-лидерах в области кибербезопасности реализованы технические и организационные инициативы, представляющие интерес для имплементации в отечественной практике.

Литература:

1. 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.
2. Цыплакова А.Д. Должностные лица и органы, обеспечивающие полноту судебной власти в арабских странах: понятие и полномочия // Вестник Дальневосточного юридического института МВД России имени И.Ф. Шилова. 2025. № 2. С. 142-151.
3. 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, 2024.
4. Elahimanesh, M., Moradi Ojghaz, M. The Role of Mother's Milk Feeding in Crime Prevention // Judgment. 2014. No. 14 (79). P. 99-119.
5. Li L., Zhou K. When content moderation is not about content: How Chinese social media platforms moderate content and why it matters // New Media & Society. 2024. DOI: 10.1177/14614448241263933.
6. Nematollahi M., Zeraat A., Ghomashi S. The Concept and Elements of Citizenship and its Role in Crime Prevention // Comparative Criminal Jurisprudence. 2021. No. 1 (2). P. 131-141.
7. Razavi Fard B., RobatJazy M., Omrani G. Prevention of Sexual Victimization in Social Networks // The Judiciarys Law Journal. 2018. No. 82 (104). P. 39-65.
8. Taslimi A.H., Ashrafy M., Malmir M. Social Prevention of Corruption // Comparative Criminal Jurisprudence. 2023. No. 3 (3). P. 1-11.
9. Tavasoli A., Poorbaferani H., Shekarchizadeh M. Comparative study of modern registration and crime prevention management in the registration system of Iran and the UAE // Culmination of Law. 2021. No. 7(3). P. 2-30.
10. Tsyplakova A.D. Comprehensive approach to cybercrime prevention in Arab countries // Law, State and Telecommunications Review. 2025. Vol. 17. No. 1. P. 23–41.
11. Ying L.X., Mohd Aman A.H., Jalil M.S., Mohd Omar T., Attarbashi Z.S., Abuzaraida M.A. Malaysia Cyber Fraud Prevention Application: Features and Functions // Asia-Pacific Journal of Information Technology and Multimedia. 2023. № 12(2). P. 312-327.
12. Zaka A.Z., Aghababai H., Shah Malekpour H. Fundamentals of Crime Prevention in Sunni Jurisprudence // Comparative Criminal Jurisprudence. 2023. No. 3 (2). P. 1-16.
13. 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. ٦٤ص.

COUNTERING CYBERCRIMES IN SOME GLOBAL SOUTH COUNTRIES: MODERN STANDING, ISSUES AND PERSPECTIVE

Introduction. *This study provides a brief overview of the current state of cybercrime response in the Global South, with a focus on the advanced practices, challenges and prospects for the development of intra-state and inter-state cooperation. The author reveals the terminology used and compares it with the national approach.*

Materials and methods. *Methodologically, the study is based on the methods of formal logic, the system method, interpretation, formal-legal, historical-legal methods, as well as methods of jurislinguistics and linguojuristics as to linguistic features of the use of terms by law enforcement officers, legislators and researchers in foreign languages. The study is comparative in nature not only as to cyber laws, but also related regulation, including by-laws and guidelines. Civil and civil procedural law are applicable as lex specialis.*

Study results. *The Global South countries are leaders in cyber security in terms of legislation, technical, organizational measures, capacity building and artificial intelligence, sometimes surpassing the regional level in cybercrime prevention. Given the development of legal regulation, cybercrime covers a wide range of areas where information and communication technologies are used. One may define cybercrimes as the use of high technology for criminal purposes, and the Global South's response focuses on criminalization and penalization, preventive measures, economic, technical and suppressive initiatives, the use of technological advances in detection and investigation, and the monitoring and filtering of illegal content.*

Discussion and conclusion. *The lack of mechanisms to review the implementation of regional conventions specifically on cybercrime, differences in the data stored by service providers and platform owners and the timeframe for their storage, in the understanding of prohibited content, and the abundance of evaluation categories can be identified as problems that should be addressed by developing an additional protocol to the UN Convention against Cybercrime and improving national regulation. The lack of a common understanding of cybercrime can be mitigated by ratifying the mentioned international treaty by Global South countries. The leading countries in the field of cyber security have implemented technical and organizational initiatives that are of interest for implementation in domestic practice.*

Alyona D. Tsyplakova,
Lecturer of the Department of Criminal Law,
Criminal Procedure and Criminology,
MGIMO University, Moscow, Russia

Ключевые слова:
противодействие преступности, киберпреступления, Глобальный Юг, незаконный контент, электронные доказательства, стратегии кибербезопасности, международное сотрудничество в борьбе с преступностью, профилактические меры, институциональные механизмы

Keywords:
crime prevention, cybercrimes, Global South, illegal content, electronic evidence, cybersecurity strategies, international cooperation on combatting in crime, preventive measures, institutional mechanisms

References:

1. Volevodz, A.G, Tsyplakova, A.D., 2025. O nekotoryh osobennostjah poluchenija cifrovyh dokazatel'stv v arabskih stranah na primere Ob#edinennyh Arabskih Jemiratov i Korolevstva Bahrejn [Regarding specific features of obtaining digital evidence in Arabic countries (the United Arab Emirates and the Kingdom of Bahrain)]. *Rossijskij sledovatel' [Russian investigator].* No 1. S. 45-49.
2. Tsyplakova A.D., 2025. Dolzhnostnye lica i organy, obespechivajushhie polnotu sudebnoj vlasti v arabskih stranah: ponjatie i polnomochija [Officials and bodies ensuring the enjoyment of the principle of the fullness of judicial power in the Arab countries: concept and powers]. *Vestnik Dal'nevostochnogo juridicheskogo instituta MVD Rossii imeni I. F. Shilova [Bulletin of the Far Eastern Law Institute of the Ministry of Internal Affairs of Russia named after I. F. Shilov].* No 2. S. 142-151.
3. Collecting Electronic Evidence in Criminal Cases in Russia and Foreign Countries: Experiences and Problems: monograph. E*d. by S.P. Shcherba (Russian ed.) and P.A. Litvishko (English ed.).* Moscow, 2024.

4. Elahimanesh, M., Moradi Ojghaz, M., 2014. The Role of Mother's Milk Feeding in Crime Prevention. *Judgment*. No. 14 (79). P. 99-119.
5. Li, L., Zhou, K., 2024. When content moderation is not about content: How Chinese social media platforms moderate content and why it matters. *New Media & Society.* DOI: 10.1177/14614448241263933.
6. Nematollahi, M., Zeraat, A., Ghomashi, S., 2021. The Concept and Elements of Citizenship and its Role in Crime Prevention. *Comparative Criminal Jurisprudence.* No. 1 (2). P. 131-141.
7. Razavi Fard, B., RobatJazy, M., Omrani, G., 2018. Prevention of Sexual Victimization in Social Networks. *The Judiciarys Law Journal.* No. 82 (104). P. 39-65.
8. Taslimi, A.H., Ashrafy, M., Malmir, M., 2023. Social Prevention of Corruption. *Comparative Criminal Jurisprudence.* No. 3 (3). P. 1-11.
9. Tavasoli, A., Poorbaferani, H., Shekarchizadeh, M., 2021. Comparative study of modern registration and crime prevention management in the registration system of Iran and the UAE. *Culmination of Law.* No. 7(3). P. 2-30.
10. Tsyplakova, A.D., 2025. Comprehensive approach to cybercrime prevention in Arab countries. *Law, State and Telecommunications Review.* Volume 17. No. 1. P. 23–41.
11. Ying, L.X., Mohd Aman, A.H., Jalil, M.S., Mohd Omar, T., Attarbashi, Z.S., Abuzaraida, M.A., 2023. Malaysia Cyber Fraud Prevention Application: Features and Functions. *Asia-Pacific Journal of Information Technology and Multimedia.* No. 12(2). P. 312-327.
12. Zaka, A. Z., Aghababai, H., Shah Malekpour, H., 2023. Fundamentals of Crime Prevention in Sunni Jurisprudence. *Comparative Criminal Jurisprudence.* No. 3 (2). P. 1-16.
13. Al'-Mardzhan, A.R., Shaki, M., Al'-Sabavi, J., Al'-Manshavi, M., Li, S., Al'-Hashel', Dz., 2024. Rukovodstvo po rabote s cifrovymi sudebno-medicinskimi dokazatel'stvami v arabskih stranah [Guidelines for Dealing with Digital Forensic Evidence in the Arab Countries].