МЕЖДУНАРОДНО-ПРАВОВЫЕ ОСНОВЫ ПРОТИВОДЕЙСТВИЯ КИБЕРПРЕСТУПНОСТИ: СООТНОШЕНИЕ УНИВЕРСАЛЬНЫХ, РЕГИОНАЛЬНЫХ И ДВУСТОРОННИХ ДОГОВОРНЫХ МОДЕЛЕЙ

Нажиматдинов Илхам Полат улы

Магистрант Университета Мировой Экономики и Дипломатии

najimatdinovilxam@gmail.com

Аннотация

Представленное научное исследование посвящено комплексному анализу эволюции и современного состояния международно-правового регулирования в сфере противодействия киберпреступности. В работе детально исследуется исторический и институциональный переход от фрагментированной системы, опирающейся на разрозненные региональные инициативы, к единому универсальному механизму, кульминацией которого стало историческое принятие Конвенции Организации Объединенных Наций против киберпреступности (Ханойской конвенции) в декабре 2024 года. Особое концептуальное внимание уделяется теоретическому и практическому разграничению трех основных подходов, доминирующих в современной международной практике: уголовно-правовой модели, модели обеспечения кибербезопасности и процессуальной модели трансграничного доступа к электронным доказательствам. В рамках исследования проводится глубокий сравнительно-правовой анализ Будапештской конвенции как первой предуниверсальной парадигмы, которая заложила основы материального права, но не смогла преодолеть барьеры государственного суверенитета. Также скрупулезно изучаются региональные правовые режимы: Малабская конвенция Африканского союза, доктринальные подходы и соглашения

Содружества Независимых Государств (СНГ) и Шанхайской организации сотрудничества (ШОС), Директива ECOWAS, а также стратегии мягкого права ОАГ и АСЕАН. Значительное место отведено анализу новейших двусторонних экзекутивных соглашений, заключаемых в рамках американского Закона CLOUD (CLOUD Act), как ответа на кризис традиционных договоров о взаимной правовой помощи (MLAT). На основе проведенного анализа обосновывается фундаментальный вывод о том, что формирование универсального режима под эгидой ООН не приведет к автоматическому вытеснению региональных и двусторонних моделей. Напротив, в глобальном праве выстраивается сложная, многоуровневая субсидиарная архитектура, в которой универсальный договор задает базовые стандарты и снимает юрисдикционные противоречия, региональные соглашения адаптируют эти стандарты под геополитическую специфику, а двусторонние инструменты обеспечивают необходимую оперативность процессуального механизма обмена цифровыми данными.

Ключевые слова: киберпреступность, Конвенция ООН, Ханойская конвенция, Будапештская конвенция, Малабская конвенция, электронные доказательства, CLOUD Act, ШОС, СНГ, ECOWAS, международное право, юрисдикция в киберпространстве.

1. Введение

В условиях стремительной цифровизации глобальной экономики, экспоненциального роста объемов обрабатываемых данных и интеграции облачных вычислений во все сферы общественной жизни киберпреступность приобрела статус одной из наиболее серьезных и разрушительных транснациональных угроз современности. Эскалация стоимости ущерба от киберпреступлений, который, по оценкам структур ООН, ежегодно обходится мировой экономике в триллионы долларов, подчеркивает настоятельную

необходимость координации международных усилий.[1] Уникальная, трансграничная природа киберпространства, характеризующаяся экстерриториальностью, анонимностью субъектов, высокой скоростью передачи информации и децентрализацией, вступила в глубокое концептуальное противоречие с традиционной Вестфальской системой международного права, всецело основанной на принципах государственного суверенитета и строгой территориальной юрисдикции.

Это противоречие породило системный кризис в механизмах расследования транснациональных преступлений и оказания взаимной правовой помощи. Как отмечает Директор Отдела по договорам Управления ООН по наркотикам и преступности (UNODC) Джон Брандолино, киберпреступность сегодня охватывает широкий спектр правонарушений, которые делятся на две обширные категории: преступления, совершаемые с использованием кибертехнологий (cyber-enabled crimes), такие как онлайн-мошенничество или торговля людьми, и специфические киберпреступления (cyber-dependent crimes), такие как создание вредоносного программного обеспечения, фишинг и атаки с использованием программ-вымогателей.[1] Вектор атак варьируется от масштабных угроз национальной безопасности, включая DDoS-атаки, до целенаправленного преследования уязвимых групп: женщин, детей, этнических и религиозных меньшинств. Статистика Специального докладчика ООН по вопросам меньшинств свидетельствует о том, что 70% и более преступлений на почве ненависти в социальных сетях направлены именно против меньшинств.[1]

Исторически международное сообщество реагировало на эту перманентно эволюционирующую угрозу сугубо реактивно и крайне фрагментарно. Отсутствие единого глобального консенсуса, обусловленное идеологическими разногласиями между ведущими геополитическими

акторами по вопросам границ информационного суверенитета, привело к формированию так называемого "лоскутного одеяла" правовых режимов. Первоначально государства полагались исключительно на адаптацию своего национального уголовного законодательства, что неизбежно создавало "юрисдикционные гавани" для киберпреступников в странах с менее развитой правовой системой. Впоследствии стали возникать региональные конвенции, наиболее значимой из которых стала Конвенция Совета Европы о киберпреступности (Будапештская конвенция) 2001 года. Однако, несмотря на ее формальную открытость для присоединения любых стран, она так и не смогла достичь статуса подлинно универсального документа ввиду серьезных политико-правовых разногласий.[2]

Возникший на глобальном уровне нормативный вакуум стимулировал появление целой плеяды субрегиональных актов (таких как Директива ECOWAS, соглашения в рамках СНГ и ШОС, Малабская конвенция Африканского союза), а также односторонних законодательных актов и двусторонних механизмов прямого экстерриториального доступа к данным (наиболее ярким примером является американский CLOUD Act). В результате современная архитектура международного сотрудничества оказалась перегружена конкурирующими нормами, несовпадающими определениями составов преступлений и различными стандартами допустимости электронных доказательств.[4]

Принятие Генеральной Ассамблеей ООН в декабре 2024 года Конвенции Организации Объединенных Наций против киберпреступности (исторически именуемой Ханойской конвенцией) ознаменовало начало совершенно нового этапа — перехода к легитимному универсальному регулированию.[5] В связи с этим центральным научным и практическим вопросом современного международного уголовного права становится уже не дискуссия о

целесообразности создания глобального договора, а глубокий анализ того, как этот новый универсальный инструмент будет соотноситься с Будапештской системой, региональными режимами и двусторонними стандартами доступа к электронным доказательствам.

2. Обзор литературы (Adabiyotlarni o'rganish)

Формирование доктринальной базы международно-правового регулирования киберпреступности характеризуется множественностью подходов. В российской и зарубежной правовой науке можно выделить несколько ключевых направлений исследований, формирующих теоретический фундамент для понимания соотношения различных договорных моделей.

Значительный вклад в осмысление универсальных и региональных механизмов борьбы с киберпреступностью внесли работы А.Г. Волеводза, который глубоко исследовал современную систему международной уголовной юстиции и правовые новации Конвенции о киберпреступности.[3] Исследователь последовательно обосновывает необходимость укрепления международного сотрудничества и создания надежных правовых основ для обмена доказательствами в электронной форме в контексте глобальных угроз.[7] Труды А.А. Данельяна и М. Иноземцева дополняют эту картину анализом международно-правового регулирования киберпространства как специфической среды, требующей пересмотра классических концепций юрисдикции.[7] П.Л. Боровик и А.А. Комаров в своих изысканиях акцентируют внимание на особенностях территориального принципа действия уголовного закона в сети Интернет и проблемах вмешательства в суверенное киберпространство, что является краеугольным камнем противоречий между Будапештской моделью и позицией государств, отстаивающих информационный суверенитет.[3]

Отдельным, критически важным направлением является исследование природы электронных доказательств. В работах А.С. Бондарева, А.П. Нагорного и А.С. Чупрова проводится исчерпывающий анализ правового статуса, допустимости, достоверности и процессуального применения цифровых (электронных) доказательств в уголовном судопроизводстве.[4] Авторы уделяют особое внимание процессуальной цепи доказательств (chain of custody), механизмам цифровой криминалистики и правовым гарантиям защиты информации.[4] Проблематика использования электронных доказательств в условиях стремительного развития цифровых технологий и социальных сетей также раскрывается в новейших исследованиях В.В. Платонова, А.П. Папикяна, Ю.А. Чич и А.В. Романова, которые указывают на существенные недостатки действующего национального законодательства перед лицом транснациональных облачных хранилищ.[4]

Зарубежная доктрина, в частности исследования, посвященные региональным режимам Глобального Юга, обращает внимание на проблему "юридической трансплантации" и недостатка институционального потенциала. Так, в работах Ученны Джерома Орджи (Uchenna Jerome Orji) проводится критический анализ правовых инструментов африканских межправительственных организаций, таких как Директива ECOWAS по киберпреступности, типовые законы COMESA и SADC, а также Малабская конвенция Африканского союза.[8] Доктрина аргументированно указывает на то, что конвенции AU часто не обеспечивают адекватной основы для взаимной правовой помощи из-за своей структурной перегруженности, что приводит к фрагментации сотрудничества по субрегиональным линиям.[8]

Таким образом, анализ научной литературы демонстрирует, что переход от регионального к универсальному уровню регулирования требует не просто компиляции существующих норм, но глубокого доктринального осмысления

различий между уголовно-правовой природой преступлений, механизмами обеспечения национальной кибербезопасности и процессуальными институтами собирания электронных доказательств.

3. Методология исследования

Настоящее исследование базируется на комплексном применении общенаучных и частнонаучных методов познания, специфичных для правовой доктрины. Основополагающим является системно-структурный метод, позволивший рассмотреть международно-правовое регулирование киберпреступности не как хаотичный набор договоров, а как многоуровневую субсидиарную систему, элементы которой (универсальные, региональные и двусторонние акты) находятся в состоянии сложного взаимодействия и взаимодополнения.

Сравнительно-правовой (компаративистский) метод применялся для сопоставления концептуальных основ различных нормативных моделей. Путем диахронного и синхронного сравнения были выявлены существенные доктринальные расхождения между подходом Совета Европы (Будапештская конвенция), интеграционными актами Африканского союза (Малабская конвенция) и подходами государств евразийского пространства (ШОС и СНГ). Формально-юридический метод использовался для детального анализа текстов международных конвенций, директив (в частности, Директивы ECOWAS 2011 года), национальных законодательных актов (CLOUD Act США, Crime (Overseas Production Orders) Act 2019 Великобритании) и Резолюций Генеральной Ассамблеи ООН (Резолюция 79/243). Синтез полученных эмпирических и нормативных данных позволил сформулировать обоснованные выводы о перспективах имплементации Ханойской конвенции в существующую архитектуру глобального цифрового права.

4. Теоретико-концептуальная дифференциация

нормативных моделей

Глубинное понимание процессов, происходящих в международном праве в сфере высоких технологий, невозможно без концептуального разграничения подходов, которые исторически смешивались, подменяли друг друга или неправомерно отождествлялись политиками и правоведами. Анализ современной доктрины и правоприменительной практики позволяет выделить три фундаментально различающиеся, хотя и тесно взаимосвязанные модели международно-правового регулирования киберпространства.

4.1. Уголовно-правовая модель (Criminal-Law Model)

Уголовно-правовая модель сфокусирована непосредственно на криминализации конкретных общественно опасных деяний и установлении процедурных рамок преследования лиц, их совершивших. Ее доктринальным ядром является материальное (субстантивное) уголовное право.[2] В рамках этой парадигмы государства на основе консенсуса договариваются о гармонизации и унификации своих национальных уголовных кодексов, устанавливая соразмерные наказания за незаконный доступ к компьютерной информации, неправомерный перехват данных, вмешательство в работу компьютерных систем, а также за мошенничество и вымогательство, совершаемые с использованием информационно-коммуникационных технологий.[10]

Эта модель требует предельно точных юридических дефиниций и строится вокруг субъекта преступления. Ярким примером реализации такой модели на субрегиональном уровне является Директива Экономического сообщества западноафриканских государств (ECOWAS) по борьбе с киберпреступностью 2011 года.[11] Данный документ императивно предписывает государствам-членам адаптировать свое субстантивное уголовное и процессуальное право.[13] В статье 1 Директивы даются

исчерпывающие определения базовым понятиям: "компьютерные данные" (любое представление фактов, информации или концепций в форме, подходящей для обработки в компьютерной системе), "компьютерная система", "электронная коммуникация", а также специфическим составам, таким как распространение расизма и ксенофобии через ИКТ и детская порнография.[13] Модель нацелена на ликвидацию пробелов в праве, чтобы действие, признаваемое преступлением в одной стране, безусловно являлось таковым и в другой, что является ключевым условием (принципом двойной криминализации) для последующей экстрадиции.[8]

4.2. Модель кибербезопасности (Cybersecurity Model)

В отличие от уголовно-правовой модели, которая по своей природе носит реактивный характер (то есть предусматривает наказание за уже совершенное правонарушение), модель кибербезопасности является превентивной, инфраструктурной и системной.[2] Она ориентирована не столько на преследование преступника, сколько на объект защиты — обеспечение бесперебойного функционирования национальной информационной инфраструктуры, устойчивости систем государственного управления и защиты интересов национальной безопасности.

Данная парадигма охватывает вопросы создания национальных стратегий защиты, формирования институциональной базы в виде правительственных центров реагирования на компьютерные инциденты (CERT/CSIRT), а также выстраивания эшелонированной защиты от государственного (и полугосударственного) шпионажа, саботажа и кибертерроризма.[8] Модель кибербезопасности наиболее ярко прослеживается в подходах Шанхайской организации сотрудничества (ШОС). В документах ШОС киберпреступность не изолируется, а рассматривается как составная часть концепции "международной информационной безопасности".[15] Страны ШОС выделяют

шесть ключевых угроз: разработка и применение "информационного оружия", информационный терроризм, киберпреступность, использование доминирующего положения в информационном пространстве в ущерб суверенитету других стран, распространение деструктивной информации (наносящей ущерб социально-политическим и духовным системам) и угрозы стабильному функционированию инфраструктур.[16]

Малабская конвенция Африканского союза также представляет собой масштабную попытку кодификации именно модели кибербезопасности на континентальном уровне, прямо предписывая создание институциональной архитектуры реагирования на угрозы в каждом государстве-члене.[14]

4.3. Модель электронных доказательств (Electronic Evidence Model)

Эта новейшая парадигма возникла как ответ на фундаментальные ограничения классического института Договоров о взаимной правовой помощи (Mutual Legal Assistance Treaties, MLAT), который в цифровую эпоху оказался критически медленным и неповоротливым.[18] Модель электронных доказательств концентрируется исключительно на процессуальных механизмах трансграничного получения цифровых следов независимо от того, было ли исходное преступление высокотехнологичным (например, хакерский взлом базы данных) или сугубо традиционным (например, организация заказного убийства или незаконный оборот наркотиков, но координируемый через зашифрованные облачные мессенджеры).

Ключевой фокус здесь направлен на разрешение коллизий юрисдикций облачных провайдеров, вопросы допустимости (admissibility) и достоверности (reliability) электронной информации в национальных судах, а также обеспечение непрерывности процессуальной цепи (chain of custody).[4] Доктрина и следственная практика сегодня сталкиваются с необходимостью оценки легитимности изъятия данных из дата-центров, расположенных в

третьих странах.[4] Именно в рамках этой модели развиваются двусторонние соглашения США в рамках Закона CLOUD и европейские инициативы (e-Evidence Regulation).[19]

Характеристика	**Уголовно-правовая модель**	**Модель кибербезопасности**	**Модель электронных доказательств**
Основной объект регулирования	Составы преступлений и санкции	Инфраструктура, национальные стратегии, суверенитет	Процессуальный доступ к данным, юрисдикция провайдеров
Характер норм	Субстантивные (материальное право)	Превентивные, организационные, институциональные	Процессуальные, экзекутивные
Ключевые институты	Двойная криминализация, экстрадиция	CERT/CSIRT, защита критической инфраструктуры	Прямые запросы провайдерам, chain of custody

Типичные примеры актов	Директива ECOWAS 2011, Будапештская конвенция (Часть I)	Соглашения ШОС, Малабская конвенция	CLOUD Act, Соглашение США-Австралия

5. Предуниверсальная парадигма: Будапештская конвенция как первая комплексная модель

До начала масштабных процессов на площадке ООН Конвенция Совета Европы о киберпреступности (Будапештская конвенция), открытая для подписания 23 ноября 2001 года, де-факто выступала в качестве золотого стандарта и предуниверсальной нормативной модели противодействия киберугрозам.[2] Ее уникальность на тот момент заключалась в том, что она впервые в истории международного права предложила целостный, структурный подход.

Конвенция объединила в себе три основополагающих столпа. Во-первых, гармонизацию материального уголовного права, обязав страны-участницы криминализировать незаконный доступ к системам, вмешательство в данные, компьютерное мошенничество, нарушения авторских прав и распространение детской порнографии. Во-вторых, реформирование уголовного процесса: документ наделял национальные правоохранительные органы специфическими, невиданными ранее полномочиями, такими как оперативное сохранение хранимых компьютерных данных (expedited preservation), обыск компьютерных систем и перехват данных о трафике в режиме реального времени. В-третьих, Конвенция заложила основы международного оперативного сотрудничества посредством создания сети круглосуточного контактного взаимодействия (сеть 24/7).

Однако, несмотря на формальную открытость Конвенции для присоединения государств, не являющихся членами Совета Европы, ее продвижение в качестве подлинно универсального инструмента столкнулось с непреодолимыми политико-правовыми и идеологическими барьерами.[2] Основная линия критики со стороны ряда крупных геополитических акторов, включая Российскую Федерацию, Китайскую Народную Республику и ряд государств Глобального Юга, выстраивалась вокруг принципиальных вопросов защиты национального суверенитета в киберпространстве.[3]

Камнем преткновения стала знаменитая статья 32 Будапештской конвенции "Трансграничный доступ к хранимым компьютерным данным с согласия или в тех случаях, когда они являются общедоступными". Положение "b" данной статьи допускало трансграничный доступ к данным без необходимости получения официального согласия государства, на территории которого эти серверы физически находились, при наличии лишь "законного и добровольного согласия лица", имеющего право раскрывать эти данные. Для государств, жестко отстаивающих модель "информационного суверенитета", такое положение рассматривалось как легализация прямого экстерриториального вмешательства иностранных спецслужб во внутренние дела и нарушение принципов Устава ООН.[3] Международный договор, по мнению ряда исследователей, должен прямо указывать на суверенитет киберпространства и абсолютную недопустимость вмешательства даже в благих целях расследования уголовных дел.[3]

Кроме того, отмечалось, что Конвенция была разработана узкой группой преимущественно развитых западных государств без учета социокультурных, технологических и правовых особенностей развивающихся стран. Эти системные противоречия привели к институциональному тупику: Будапештская конвенция, безусловно, стала высокоэффективным рабочим

инструментом для группы стран-единомышленников, но не смогла эволюционировать в инклюзивную глобальную платформу. Это историческое ограничение объективно предопределило необходимость запуска нового переговорного процесса под эгидой более широкой структуры — Организации Объединенных Наций.

6. Конвенция ООН против киберпреступности (Ханойская конвенция) как новый универсальный режим

Осознание пределов масштабируемости региональных режимов и нарастающая интенсивность транснациональных кибератак привели международное сообщество к императивной необходимости разработки подлинно универсального документа, базирующегося на консенсусе всех 193 государств-членов ООН.[6] Результатом многолетних, сложнейших дипломатических усилий, длившихся более четырех лет, стало принятие Генеральной Ассамблеей ООН 24 декабря 2024 года Конвенции Организации Объединенных Наций против киберпреступности на основании Резолюции 79/243.[5]

6.1. Структурные инновации и охват Конвенции

Принятый документ, ставший первым глобальным международным договором ООН по данной проблематике за последние 20 лет, представляет собой монументальный правовой акт, состоящий из 9 глав и 71 статьи.[6] Его архитектура отражает ювелирный компромисс между правоохранительными интересами государств, абсолютными императивами защиты суверенитета и необходимостью обеспечения базовых прав человека в цифровой среде.[23]

Документ криминализирует беспрецедентно широкий спектр деяний. Как отмечает майор Фам Куанг Хи из Министерства общественной безопасности Вьетнама, Ханойская конвенция вводит в международно-правовой оборот понятия целого ряда новых видов преступлений, которые ранее никогда не

регламентировались на столь высоком уровне: от несанкционированного доступа и вмешательства в системы до сложнейших форм интернет-мошенничества.[24] Важнейшей социальной инновацией Конвенции является ее фокусировка на защите уязвимых категорий лиц. В документе подчеркивается непропорционально негативное воздействие сетевых преступлений на женщин, детей, а также пресекается деятельность, связанная с онлайн-терроризмом, торговлей людьми через интернет, контрабандой наркотиков и масштабными финансовыми преступлениями.[25]

Одним из главных прорывов документа стала глубокая проработка вопросов сбора и обмена электронными доказательствами. В отличие от узкорегиональных актов, Конвенция ООН устанавливает глобальные механизмы для расследования и передачи электронных доказательств не только по сугубо высокотехнологичным посягательствам, но и в отношении любых серьезных преступлений (serious crimes, определяемых как деяния, наказуемые лишением свободы на срок не менее четырех лет), если цифровые следы имеют ключевое значение для следствия.[5]

6.2. Баланс суверенитета, прав человека и сотрудничества

Главным политическим фактором, позволившим достичь беспрецедентного консенсуса в рамках Генеральной Ассамблеи ООН, стал жесткий акцент на уважении суверенного равенства государств и принципа невмешательства во внутренние дела.[3] Концептуально противостоя подходу Будапештской конвенции, Конвенция ООН категорически отвергает механизмы прямого одностороннего проникновения в зарубежные компьютерные сети национальными правоохранительными органами. Все процедуры сбора и передачи данных строго подчинены официальным каналам взаимной помощи с обязательным соблюдением конституционных принципов и материального права запрашиваемого государства. Это положение нашло

свое подтверждение, например, в декларации Вьетнама о том, что положения Конвенции не являются самоисполнимыми (non-self-executing) и подлежат имплементации исключительно на основе внутреннего права и принципа взаимности.[21]

При этом Конвенция создает современный "круглосуточный механизм сотрудничества", институционализирующий обмен оперативной информацией, одновременно обеспечивая гарантии соблюдения прав человека.[21] Генеральный секретарь ООН Антониу Гутерриш подчеркнул, что Конвенция создает "беспрецедентную платформу для сотрудничества", защищающую жертв и права человека в сети.[25] Важнейшим условием поддержки договора со стороны развивающихся стран (Глобального Юга) стало включение масштабных положений о технической помощи (technical assistance) и наращивании потенциала (capacity building), направленных на ликвидацию технологического разрыва между государствами.[25]

6.3. Геополитическое значение "Ханойского этапа"

Согласно статье 64 документа, Конвенция открывается для официального подписания 25–26 октября 2025 года в городе Ханой (Социалистическая Республика Вьетнам), после чего она продолжит быть открытой для присоединения в штаб-квартире ООН в Нью-Йорке до 31 декабря 2026 года.[21] Ввиду этого исторического факта договор получит устойчивое международное наименование "Ханойская конвенция".[6] Конвенция вступит в силу через 90 дней после ратификации сороковым государством.[5]

Выбор Вьетнама в качестве площадки для подписания имеет глубочайшее геополитическое и дипломатическое значение. Проведение торжественной церемонии и Саммита под девизом «Борьба с киберпреступностью – совместная ответственность – обеспечение нашего будущего» с участием Президента Вьетнама Лыонг Кыонга и Генерального секретаря ООН

символизирует смещение центра тяжести глобальной технологической дипломатии в сторону Азиатско-Тихоокеанского региона.[23] Как отметил вице-премьер, министр иностранных дел Вьетнама Буй Тхань Шон, впервые в 47-летней истории партнерства страны с ООН многосторонний договор столь высокого уровня носит имя вьетнамского города.[6] Мероприятие, собирающее представителей более 100 стран, технологических компаний и международных организаций, закрепляет фундаментальную парадигму: киберпространство является общим достоянием человечества, защита которого возможна исключительно при солидарном разделении ответственности между всеми участниками международного сообщества.[24]

7. Региональные договорные модели в контексте глобализации: специфика, достижения и пределы

Длительная разработка универсальной Конвенции ООН происходила отнюдь не в правовом вакууме, а на фоне уже сформировавшихся и функционирующих региональных экосистем. Глубокий анализ показывает, что эти региональные инициативы не были просто попытками скопировать Будапештскую систему; они эволюционировали как специфические, аутентичные правовые инструменты, отражающие уникальные социально-экономические, культурные реалии и угрозы своих континентов.

7.1. Африканский союз: Малабская конвенция и субрегиональные инициативы

В 2014 году на 23-й Очередной сессии Африканского союза в Экваториальной Гвинее была принята Конвенция о кибербезопасности и защите персональных данных (широко известная как Малабская конвенция).[12] Данный инструмент был амбициозно призван модернизировать уголовно-правовые институты континента и стать ответом на феноменальный рост проникновения интернета в Африке.[8]

Уникальной и одновременно самой доктринально уязвимой чертой Малабской конвенции стала ее структура. Документ был разделен на три взаимосвязанные, но концептуально разнородные главы, попытавшись объединить в одном акте регулирование электронных транзакций, защиту персональных данных, кибербезопасность и борьбу с киберпреступностью.[9] Конвенция прямо обязывает государства разработать национальные стратегии кибербезопасности, учредить механизмы реагирования на инциденты и принять законы, карающие за деяния, посягающие на конфиденциальность и доступность систем.[12]

Однако стремление "объять необъятное" (в отличие от европейского подхода, где защита персональных данных регулируется отдельным сложнейшим регламентом GDPR, а преступность — Будапештской конвенцией) привело к серьезным проблемам с ратификацией и имплементацией.[9] Эксперты отмечают, что дефиниции Малабской конвенции оказались менее детализированными, чем в европейских аналогах, что создает препятствия для двойной криминализации при взаимной правовой помощи.[9] Как следствие, процесс вступления документа в силу затянулся почти на десятилетие. Статья 36 требовала ратификации как минимум 15 государствами-членами, и этот порог был достигнут лишь после присоединения Мавритании, что позволило конвенции вступить в силу только 8 июня 2023 года (в марте 2023 года конвенцию подписал также Судан).[17]

Осознавая медлительность континентальных процессов Африканского союза, отдельные интеграционные блоки создали более оперативные и сфокусированные субрегиональные механизмы. Экономическое сообщество западноафриканских государств (ECOWAS) приняло в 2010 году Дополнительный акт о защите персональных данных, а в 2011 году — Директиву по борьбе с киберпреступностью.[11] Директива ECOWAS ставит

перед странами региона ряд стратегических задач: от принятия материальных и процессуальных норм до создания минимального национального потенциала расследований, гармонизации институциональных структур защиты критических инфраструктур и продвижения культуры кибербезопасности.[35] Аналогичные процессы шли на юге континента, где Сообщество развития Юга Африки (SADC) в 2012 году утвердило Типовой закон SADC о киберпреступности.[8]

7.2. Евразийское пространство: стратегическая суверенная модель СНГ и ШОС

Совершенно иной доктринальный подход, продиктованный геополитическими императивами, сформировался на евразийском пространстве. Страны Содружества Независимых Государств (СНГ) и Шанхайской организации сотрудничества (ШОС) с самого начала выстраивали регулирование не вокруг наделения полиции наднациональными процессуальными правами, а вокруг жесткой защиты национальной безопасности и государственного суверенитета в информационном пространстве.

В рамках ШОС (основанной Китаем, Россией, Казахстаном, Кыргызстаном, Таджикистаном и др.) проблема киберпреступности никогда не рассматривалась в отрыве от глобальной парадигмы "международной информационной безопасности" (International Information Security).[15] Еще в Екатеринбургской декларации 2009 года и коммюнике в Душанбе 2008 года государства ШОС выражали обеспокоенность применением ИКТ в целях, несовместимых с международной стабильностью.[15] Ключевой документ ШОС выделяет шесть угроз, где киберпреступность стоит в одном ряду с подготовкой к информационной войне, информационным терроризмом и

вмешательством во внутренние дела через распространение деструктивной социокультурной информации.[16]

На уровне СНГ системной вехой стало Соглашение о сотрудничестве государств-участников СНГ в борьбе с преступлениями в сфере информационных технологий, подписанное 28 сентября 2018 года в Душанбе (ратифицировано Президентом РФ в июле 2021 года).[36] Данное соглашение регламентирует процедуры предупреждения, выявления и расследования преступлений с бескомпромиссной опорой на национальное законодательство сторон, исключая любые лазейки для экстерриториального вмешательства в сети суверенных государств без прямого межправительственного запроса.[36]

7.3. Интеграционные парадигмы ОАГ и АСЕАН

В Западном полушарии Организация американских государств (ОАГ) сделала основную ставку не на жесткое кодифицирование, а на модель "мягкого права" (soft law) и наращивание институционального потенциала (capacity building). Вместо разработки собственной панамериканской конвенции, ОАГ сосредоточилась на технической поддержке стран Латинской Америки, помогая им модернизировать национальные законы и интегрироваться во внешние рамки, часто с оглядкой на Будапештскую систему.

Ассоциация государств Юго-Восточной Азии (АСЕАН), напротив, применяет компромиссную, эволюционную модель. Регион характеризуется колоссальным дисбалансом в уровне технологического и экономического развития стран-членов. Политика АСЕАН в области кибербезопасности исторически ориентировалась на принятие добровольных, неимперативных норм ответственного поведения государств в киберпространстве с постепенным, крайне осторожным переходом к более строгим уголовно-правовым механизмам координации полицейских расследований.

Наименование акта	**Юрисдикция**	**Год принятия**	**Ключевая особенность**
Директива ECOWAS	Западная Африка	2011	Обязательная гармонизация уголовного права, детальные дефиниции
Малабская конвенция	Африканский союз	2014	Интеграция киберпреступности, защиты данных и е-коммерции в один акт
Соглашение СНГ	Евразия	2018	Строгий приоритет национального суверенитета при расследовании ИТ-преступлений

Ханойская конвенция	Весь мир (ООН)	2024	Первая подлинно универсальная криминализация и механизм электронных доказательств

8. Двусторонние соглашения и модель прямого доступа к электронным доказательствам

Одной из самых острых проблем современного международного процессуального права, которая долгое время оставалась "слепым пятном" конвенциональных механизмов, является оперативный доступ к электронным доказательствам. Цифровые следы обладают уникальным свойством: они физически хранятся на серверах корпораций в одной юрисдикции (чаще всего в США или Ирландии), но критически необходимы для расследования преступления, совершенного в совершенно другой стране.[4] Классическая, освященная веками процедура исполнения Договоров о взаимной правовой помощи (MLAT) требует прохождения запроса через цепочку дипломатических и прокурорских инстанций обеих стран, что на практике занимает от 6 до 24 месяцев.[18] Для цифровых данных, которые могут быть стерты или зашифрованы злоумышленником за доли секунды, такая задержка фатальна для правосудия.

8.1. Закон CLOUD: Реформирование Закона о хранимых коммуникациях

Для преодоления этого процедурного кризиса Соединенные Штаты Америки, являющиеся юрисдикцией базирования подавляющего большинства глобальных IT-корпораций (Google, Meta, Microsoft, Apple), в марте 2018 года

приняли "Закон об уточнении правомерного использования данных за рубежом" (Clarifying Lawful Overseas Use of Data Act — CLOUD Act).[18] Принятие этого акта было не просто теоретической инициативой, а прямым ответом правовой системы на резонансное дело "Microsoft Ireland". В рамках этого кейса корпорация Microsoft успешно оспорила в суде легитимность американского ордера на изъятие электронных писем пользователя, хранящихся в дата-центре в Дублине, утверждая, что юрисдикция США не распространяется на территорию Ирландии.[18]

Закон CLOUD радикально изменил правовую реальность, преследуя две фундаментальные цели. Во-первых, он внес изменения в положения Закона о хранимых коммуникациях (Stored Communications Act, кодифицировано как 18 U.S.C. § 2713). Согласно новой редакции, американские провайдеры электронных услуг обязаны предоставлять данные, находящиеся в их владении или под их контролем, по законному ордеру правоохранительных органов США "независимо от того, находятся ли такие сообщения, записи или иная информация внутри или за пределами территории Соединенных Штатов".[18] Это законодательно аннулировало аргументацию по делу Microsoft Ireland.

8.2. Экзекутивные двусторонние соглашения как новый стандарт

Во-вторых, и это имеет грандиозное значение для международного права, CLOUD Act наделил правительство США полномочиями заключать беспрецедентные по своей природе двусторонние экзекутивные соглашения (executive agreements) с "надежными" иностранными государствами.[18]

Эти соглашения создают революционную процессуальную модель. Они заранее квалифицируют иностранные правоохранительные органы, позволяя им напрямую обращаться к американским IT-провайдерам с обязательными к

исполнению ордерами за электронными доказательствами, полностью обходя громоздкий правительственный аппарат MLAT.[18]

Первым историческим прецедентом стала реализация Соглашения между США и Великобританией (Agreement on Access to Electronic Data for the Purpose of Countering Serious Crime), которое вступило в силу 8 июля 2020 года.[18] В рамках имплементации этого партнерства Великобритания приняла собственный профильный закон — Crime (Overseas Production Orders) Act 2019, который дарит британской полиции, прокуратуре и следственным органам право направлять предписания напрямую американским компаниям при расследовании серьезных преступлений.[38] 15 декабря 2021 года аналогичное высокоэффективное двустороннее соглашение было подписано между правительствами Соединенных Штатов и Австралии, окончательно закрепляя этот механизм в качестве нового золотого стандарта ускоренного трансграничного обмена доказательствами в англосаксонской правовой семье.[19]

Параллельно Европейский Союз активно разрабатывает и внедряет собственную систему внутреннего регулирования (e-Evidence Regulation), стремясь, с одной стороны, гармонизировать получение данных внутри юрисдикций ЕС, а с другой — выстроить мощный коллективный канал равноправного взаимодействия с американским режимом CLOUD Act.[20] В контексте универсализации международного права эта модель экзекутивных двусторонних соглашений рассматривается не как идеологический конкурент глобальным конвенциям ООН, а как их узкоспециализированный, высокоскоростной процессуальный инструмент, обеспечивающий необходимую динамику правосудия.

9. Синтез архитектуры будущего: универсализация без полного вытеснения региональных режимов

Принятие Ханойской конвенции ООН неизбежно ставит перед мировым юридическим сообществом сложнейший научный и практический вопрос: какова судьба и функциональная роль существующих региональных актов и двусторонних соглашений в условиях глобального универсального режима? Историко-правовой анализ развития институтов международного права (по аналогии с Конвенциями ООН против коррупции или транснациональной организованной преступности) позволяет с высокой долей научной уверенности утверждать, что формирование универсального режима в сфере киберпреступности не приведет к полной аннигиляции фрагментированной системы. Напротив, мировая архитектура переходит в стадию глубокой стратификации, специализации и субсидиарности.

Во-первых, Конвенция ООН, став фундаментальным, неоспоримым базисом, обеспечит общий юридический знаменатель для всех 193 стран мира. Она концептуально решит глобальную проблему "юрисдикционных оазисов", принудив даже самые малые и технологически слабые государства принять минимально необходимый, стандартизированный пакет уголовных законов и алгоритмов взаимодействия при сборе электронных доказательств.[5] Это имеет колоссальное значение для стран, которые принципиально не присоединялись к Будапештской конвенции ввиду опасений за свой информационный суверенитет, но всецело готовы сотрудничать под эгидой легитимных механизмов ООН и на условиях консенсуса.[2] В данном аспекте Конвенция ООН выступает как lex generalis (общий закон).

Во-вторых, региональные конвенции и соглашения (такие как Малабская конвенция, акты СНГ и ШОС, Директивы ECOWAS) безусловно продолжат функционировать, эволюционируя для выполнения задач более тонкой институциональной настройки. Универсальный глобальный договор ООН в силу своей компромиссной природы физически не может охватить

специфические, узкорегиональные аспекты национальной безопасности. Например, он не может предписать глубокую интеграцию систем защиты критической инфраструктуры с военными доктринами государств (что является предметом регулирования ШОС), или детализировать создание совместных континентальных центров реагирования (CSIRT), что прямо предусмотрено стратегиями Африканского союза и ECOWAS.[14] Региональные договоры будут гармонично дополнять механизм ООН по принципу lex specialis derogat legi generali (специальный закон отменяет действие общего), адаптируя общие глобальные нормы к сложным культурным, экономическим, политическим и правовым реалиям конкретных макрорегионов. Сама Конвенция ООН не только не запрещает, но и прямо предусматривает и поощряет возможность заключения странами двусторонних и многосторонних соглашений для более эффективной имплементации своих базовых положений.[21]

В-третьих, процессуальная сфера, касающаяся немедленного, санкционированного доступа к электронным доказательствам (electronic evidence) у частных транснациональных технологических гигантов, по-прежнему будет всецело тяготеть к гибким двусторонним исполнительным соглашениям (развивающимся по модели CLOUD Act). Универсальная конвенция ООН задает незыблемые принципы обмена доказательствами по линии G2G (правительство — правительство) с соблюдением всех дипломатических протоколов. В то же время двусторонние договоры создают инновационные, защищенные механизмы прямого взаимодействия типа G2B (иностранное правительство — частная корпорация в другой юрисдикции).[37] Высочайший уровень доверия, необходимый для предоставления следственным органам одной страны прямого доступа к серверам корпораций другой страны, может быть обеспечен исключительно на основе точечных двусторонних договоренностей стран с предельно схожими правовыми

демократическими стандартами и надежной системой защиты персональных данных.[19]

10. Выводы (Xulosalar)

Ретроспективный и системный анализ международно-правовых основ противодействия киберпреступности выявляет чрезвычайно сложную, нелинейную динамику перехода глобальной системы от состояния глубокой институциональной фрагментации к многоуровневой функциональной гармонизации. На протяжении долгих лет мировая юридическая архитектура находилась в состоянии разрозненности: Будапештская конвенция заложила прочную уголовно-правовую доктринальную основу, но столкнулась с непреодолимыми барьерами суверенного неприятия со стороны крупных акторов; многочисленные региональные инициативы, такие как амбициозная Малабская конвенция Африканского союза и концептуальные стандарты ШОС, пытались внедрить комплексную модель кибербезопасности, но регулярно страдали от трудностей практической имплементации и нехватки технологического потенциала; а точечные двусторонние инициативы, такие как американский Закон CLOUD, предложили прагматичные, молниеносные, но весьма избирательные решения острейшей проблемы трансграничного доступа к электронным доказательствам.

Подписание Ханойской конвенции ООН, запланированное на 2025 год, без преувеличения является эпохальным событием, открывающим совершенно новую главу в поступательном развитии глобального международного права.[6] Этот уникальный документ впервые в истории человечества объединил интересы технологически развитых держав Глобального Севера и развивающихся стран Глобального Юга. Конвенция предложила исчерпывающую, сбалансированную нормативную модель, которая криминализирует широчайший спектр высокотехнологичных деяний

в глобальном масштабе, создает универсальные, легитимные правила процессуального обращения с электронными доказательствами и, что принципиально важно, обеспечивает безусловную нерушимость государственного суверенитета и территориальной юрисдикции.

При этом грядущая эра универсализации отнюдь не означает отказа от накопленного исторического опыта. Будущая система будет носить ярко выраженный гибридный характер: Конвенция ООН станет конституирующим ядром, задающим единые легитимные стандарты криминализации и международного сотрудничества; региональные договоры (СНГ, ШОС, акты АСЕАН, ОАГ и Африканского союза) будут выступать жизненно важными инструментами глубокой интеграции политик кибербезопасности и институциональной гармонизации; а гибкие двусторонние соглашения о доступе к данным останутся скоростными процессуальными магистралями для эффективной оперативной работы правоохранительных органов. Только такой сложный, глубоко интегрированный симбиоз универсальных, региональных и двусторонних моделей способен обеспечить подлинно эффективную защиту мирового цифрового пространства, национальных экономик и прав личности в условиях перманентно эволюционирующих угроз XXI века.

Источники

1. Basic facts about the global cybercrime treaty - the United Nations, дата последнего обращения: июня 12, 2026, https://www.un.org/en/peace-and-security/basic-facts-about-global-cybercrime-treaty

2. На правах рукописи Пучков Денис Валентинович УГОЛОВНО-ПРАВОВАЯ МОДЕЛ - Уральский государственный юридический университет, дата последнего обращения: июня 12, 2026, https://www.usla.ru/science/dissovet/file/base/7/546/autoabstract_dl.pdf

3. Международно-правовая регламентация ответственности за киберпреступления Текст научной статьи по специальности «Право - КиберЛенинка, дата последнего обращения: июня 12, 2026, https://cyberleninka.ru/article/n/mezhdunarodno-pravovaya-reglamentatsiya-otvetstvennosti-za-kiberprestupleniya

4. ЭЛЕКТРОННЫЕ ДОКАЗАТЕЛЬСТВА В УГОЛОВНОМ ПРОЦЕССЕ НА СОВРЕМЕННОМ ЭТАПЕ Текст научной статьи по специальности «Право - КиберЛенинка, дата последнего обращения: июня 12, 2026, https://cyberleninka.ru/article/n/elektronnye-dokazatelstva-v-ugolovnom-protsesse-na-sovremennom-etape

5. United Nations Convention against Cybercrime | Eurojust - European Union, дата последнего обращения: июня 12, 2026, https://www.eurojust.europa.eu/publication/united-nations-convention-against-cybercrime

6. Official Statement - The United Nations Convention, дата последнего обращения: июня 12, 2026, https://hanoiconvention.org/official-statement/

7. конвенция организации объединенных наций ... - Публикации ВШЭ, дата последнего обращения: июня 12, 2026, https://publications.hse.ru/pubs/share/direct/1043679582.pdf

8. Multilateral Legal responses to cyber Security in Africa: Any Hope for Effective International cooperation? | CCDCOE, дата последнего обращения: июня 12, 2026, https://ccdcoe.org/uploads/2018/10/Art-08-Multilateral-Legal-Responses-to-Cyber-Security-in-Africa-Any-Hope-for-Effective-International-Cooperation.pdf

9. Full article: Cyber governance in Africa: at the crossroads of politics, sovereignty and cooperation - Taylor & Francis, дата последнего обращения: июня 12, 2026, https://www.tandfonline.com/doi/full/10.1080/25741292.2023.2199960

10. UN Cybercrime Convention - Full Text - UNODC, дата последнего обращения: июня 12, 2026, https://www.unodc.org/unodc/en/cybercrime/convention/text/convention-full-text.html

11. Cybercrime Module 3 Key Issues: International and Regional Instruments - UNODC, дата последнего обращения: июня 12, 2026, https://www.unodc.org/cld/es/education/tertiary/cybercrime/module-3/key-issues/international-and-regional-instruments.html

12. Regulating Digital Data in Africa - Open Knowledge Repository, дата последнего обращения: июня 12, 2026, https://openknowledge.worldbank.org/bitstreams/62e27761-1da1-467f-99a2-a6a1a3cf3b54/download

13. economic community of - UNIDIR Cyber Policy Portal Database, дата последнего обращения: июня 12, 2026, https://database.cyberpolicyportal.org/api/files/1663937573131gpbf0y5zbu.pdf

14. THE MALABO ROADMAP - Data Protection Africa, дата последнего обращения: июня 12, 2026, https://dataprotection.africa/wp-content/uploads/malabo_roadmap_Sept_2022.pdf

15. SCO - Cybercrime Law, дата последнего обращения: июня 12, 2026, https://www.cybercrimelaw.net/SCO.html

16. Agreement on Cooperation in Ensuring International Information Security between the Member States of the Shanghai Cooperation Organization, дата последнего обращения: июня 12, 2026, https://eng.sectsco.org/files/207508/207508

17. Malabo Convention - Wikipedia, дата последнего обращения: июня 12, 2026, https://en.wikipedia.org/wiki/Malabo_Convention

18. The CLOUD Act | Strategic Technologies Blog - CSIS, дата последнего обращения: июня 12, 2026, https://www.csis.org/blogs/strategic-technologies-

blog/cloud-act

19. CLOUD Act Resources - Criminal Division - Department of Justice, дата последнего обращения: июня 12, 2026, https://www.justice.gov/criminal/cloud-act-resources

20. Navigating Toward an EU-U.S. Agreement on Electronic Evidence - Lawfare, дата последнего обращения: июня 12, 2026, https://www.lawfaremedia.org/article/navigating-toward-an-eu-u.s.-agreement-on-electronic-evidence

21. United Nations Convention against Cybercrime - UNTC, дата последнего обращения: июня 12, 2026, https://treaties.un.org/pages/ViewDetails.aspx?src=TREATY&mtdsg_no=XVIII-16&chapter=18&clang=_en

22. United Nations Convention against Cybercrime - UNODC, дата последнего обращения: июня 12, 2026, https://www.unodc.org/unodc/en/cybercrime/convention/home.html

23. Открытие церемонии подписания Конвенции ООН против киберпреступности, дата последнего обращения: июня 12, 2026, https://ru.vietnamplus.vn/otkritie-tseremonii-podpisanija-konventsii-oon-protiv-kiberprestupnosti-post86732.vnp

24. Вьетнам разделяет ответственность с международным сообществом за защиту киберпространства - VOV, дата последнего обращения: июня 12, 2026, https://vov.vn/ru-RU/%D0%92%D1%8C%D0%B5%D1%82%D0%BD%D0%B0%D0%BC%D1%80%D0%B0%D0%B7%D0%B4%D0%B5%D0%BB%D1%8F%D0%B5%D1%82%D0%BE%D1%82%D0%B2%D0%B5%D1%82%D1%81%D1%82%D0%B2%D0%B5%D0%BD%D0%BD%D0%BE%D1%81%D1%82%D1%8C%D1%81%D0%BC%D0%B5%D0%B6%D0%B4%D1%83%D0%BD%D0%B0%D1%80%D0%BE%D0%B4%D0%BD%D1%8B%D0%BC%D1%81%D0%BE%D0%BE%D0

%B1%D1%89%D0%B5%D1%81%D1%82%D0%B2%D0%BE%D0%BC%D0%B7%D0%B0%D0%B7%D0%B0%D1%89%D0%B8%D1%82%D1%83%D0%BA%D0%B8%D0%B1%D0%B5%D1%80%D0%BF%D1%80%D0%BE%D1%81%D1%82%D1%80%D0%B0%D0%BD%D1%81%D1%82%D0%B2%D0%B0-1257492.vov

25. UN General Assembly adopts milestone cybercrime treaty - UN News, дата последнего обращения: июня 12, 2026, https://news.un.org/en/story/2024/12/1158521

26. Конвенция ООН против киберпреступности - Vietnam.vn, дата последнего обращения: июня 12, 2026, https://www.vietnam.vn/ru/cong-uoc-lhq-ve-chong-toi-pham-mang

27. Ханойская конвенция создает глобальную правовую основу для борьбы с киберпреступностью - Báo Ảnh Việt Nam, дата последнего обращения: июня 12, 2026, https://vietnam.vnanet.vn/russian/tin-van/%D1%85%D0%B0%D0%BD%D0%BE%D0%B8%D1%81%D0%BA%D0%B0%D1%8F-%D0%BA%D0%BE%D0%BD%D0%B2%D0%B5%D0%BD%D1%86%D0%B8%D1%8F-%D1%81%D0%BE%D0%B7%D0%B4%D0%B0%D0%B5%D1%82-%D0%B3%D0%BB%D0%BE%D0%B1%D0%B0%D0%BB%D1%8C%D0%BD%D1%83%D1%8E-%D0%BF%D1%80%D0%B0%D0%B2%D0%BE%D0%B2%D1%83%D1%8E-%D0%BE%D1%81%D0%BD%D0%BE%D0%B2%D1%83-%D0%B4%D0%BB%D1%8F-%D0%B1%D0%BE%D1%80%D1%8C%D0%B1%D1%8B-%D1%81-%D0%BA%D0%B8%D0%B1%D0%B5%D1%80%D0%BF%D1%80%D0%B5%D1%81%D1%82%D1%83%D0%BF%D0%BD%D0%BE%D1%81%D1%82%D1%8C%D1%8E-412076.html

28. Церемония подписания Конвенции ООН против киберпреступности

открывается сегодня в Ханое - ИЛЛЮСТРИРОВАННЫЙ ЖУРНАЛ ВЬЕТНАМ НА РУССКОМ ЯЗЫКЕ, дата последнего обращения: июня 12, 2026, https://vietnam.vnanet.vn/russian/print/%D1%86%D0%B5%D1%80%D0%B5%D0%BC%D0%BE%D0%BD%D0%B8%D1%8F-%D0%BF%D0%BE%D0%B4%D0%BF%D0%B8%D1%81%D0%B0%D0%BD%D0%B8%D1%8F-%D0%BA%D0%BE%D0%BD%D0%B2%D0%B5%D0%BD%D1%86%D0%B8%D0%B8-%D0%BE%D0%BE%D0%BD-%D0%BF%D1%80%D0%BE%D1%82%D0%B8%D0%B2-%D0%BA%D0%B8%D0%B1%D0%B5%D1%80%D0%BF%D1%80%D0%B5%D1%81%D1%82%D1%83%D0%BF%D0%BD%D0%BE%D1%81%D1%82%D0%B8-%D0%BE%D1%82%D0%BA%D1%80%D1%8B%D0%B2%D0%B0%D0%B5%D1%82%D1%81%D1%8F-%D1%81%D0%B5%D0%B3%D0%BE%D0%B4%D0%BD%D1%8F-%D0%B2-%D1%85%D0%B0%D0%BD%D0%BE%D0%B5-412557.html

29. Data Privacy and Data Protection - sub-Saharan Africa - Media Defence, дата последнего обращения: июня 12, 2026, https://www.mediadefence.org/resource-hub/data-privacy-protection-sub-saharan-africa/

30. Data Protection Legal Regime and Data Governance in Africa: An Overview, дата последнего обращения: июня 12, 2026, https://publication.aercafricalibrary.org/bitstreams/0f32a360-2532-46dc-8b1d-62d4ac5411e5/download

31. AFRICAN UNION CONVENTION ON CYBER SECURITY AND PERSONAL DATA PROTECTION, дата последнего обращения: июня 12, 2026, https://ccdcoe.org/uploads/2018/11/AU-270614-CSConvention.pdf

32. The AU can help African countries adopt the UN cybercrime convention. But

the challenges are significant | Chatham House, дата последнего обращения: июня 12, 2026, https://www.chathamhouse.org/2025/10/au-can-help-african-countries-adopt-un-cybercrime-convention-challenges-are-significant

33. The African Union's Malabo Convention on Cyber Security and Personal Data Protection enters into force nearly after a decade. What does it mean for Data Privacy in Africa or beyond? - EJIL: Talk!, дата последнего обращения: июня 12, 2026, https://www.ejiltalk.org/the-african-unions-malabo-convention-on-cyber-security-and-personal-data-protection-enters-into-force-nearly-after-a-decade-what-does-it-mean-for-data-privacy-in-africa-or-beyond/

34. How can the legal framework provide safeguards against the misuse of data?, дата последнего обращения: июня 12, 2026, https://www.migrationdataportal.org/handbooks/chapter-3-data-regulatory-environment/how-can-legal-framework-provide-safeguards-against

35. ECOWAS Regional Cybersecurity and Cybercrime Strategy - Digital Watch Observatory, дата последнего обращения: июня 12, 2026, https://dig.watch/resource/ecowas-regional-cybersecurity-and-cybercrime-strategy

36. Law ratifying Agreement on cooperation of the CIS member states in the fight against cybercrimes - President of Russia, дата последнего обращения: июня 12, 2026, http://en.kremlin.ru/acts/news/65986

37. The CLOUD Act, Explained, дата последнего обращения: июня 12, 2026, https://www.orrick.com/en/Insights/2018/04/The-CLOUD-Act-Explained

38. The CLOUD Act Data Access Agreement – 10 Things That U.S. Telecommunications Companies Need to Know Now - Wiley Rein, дата последнего обращения: июня 12, 2026, https://www.wiley.law/alert-The-CLOUD-Act-Data-Access-Agreement-10-Things-That-US-Telecommunications-Companies-Need-to-Know-Now