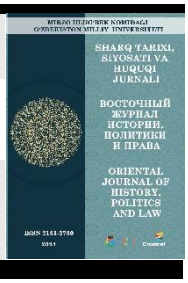
**DOI:** https://doi.org/10.37547/supsci-ojhpl-06-11-26 **Pages: 306-320**

Oriental Journal of History, Politics and Law

SUPPORT SCIENCE

**ORIENTAL JOURNAL OF HISTORY, POLITICS AND LAW**

journal homepage:
https://www.supportscience.uz/index.php/ojhpl




# CYBERCRIME IN INTERNATIONAL LAW: CONCEPT AND LEGAL NATURE

***Shukhrat Atakhanov***
*Independent researcher*

## ABOUT ARTICLE

**Key words:** cybercrime; crimes in the sphere of information technology; UN Convention against Cybercrime; Budapest Convention; international cooperation; electronic evidence; information security; Republic of Uzbekistan; transborder nature; criminal jurisdiction.

**Received:** 12.11.26
**Accepted:** 13.11.26
**Published:** 14.11.26

**Abstract:** The article examines the concept and legal nature of cybercrime as a multilevel category of international law. The purpose of the study is to identify the definitional foundation of international cooperation between states in combating crimes committed through the use of information and communication technologies, and to determine the directions for harmonizing the national legislation of the Republic of Uzbekistan with the 2024 United Nations Convention against Cybercrime. The methodological framework of the research comprises historical-legal, comparative-legal, systemic and formal-dogmatic methods, as well as the analysis of international treaties at the universal, regional and integration levels. It is demonstrated that the terminological evolution from “computer crime” to “cybercrime” and further to “AI-related offences” reflects the consistent expansion of the subject matter of international legal regulation following the technological architecture of infringements. The article substantiates the thesis that the legal nature of cybercrime is determined not by a single definition, but by the architecture of three treaty layers: the universal (UN Convention of 2024), the regional (Budapest Convention of 2001) and the integration (CIS and SCO instruments) ones. Criteria for delimiting cybercrime, cyberterrorism and military cyber operations are proposed. Four terminological dissonances between the national law of the Republic of Uzbekistan and the universal

standard are identified, and an author's definition of cybercrime in the international legal aspect, suitable for implementation into the legislation of the Republic of Uzbekistan, is formulated.

# XALQARO HUQUQDA KIBERJINOYATCHILIK: TUSHUNCHASI VA HUQUQIY MOHIYATI

***Shuxrat Ataxanov***
*Mustaqil izlanuvchi*

## MAQOLA HAQIDA

**Kalit so‘zlar:** kiberjinoyatchilik; axborot texnologiyalari sohasidagi jinoyatlar; BMTning Kiberjinoyatchilikka qarshi konvensiyasi; Budapesht konvensiyasi; xalqaro hamkorlik; elektron dalillar; axborot xavfsizligi; O‘zbekiston Respublikasi; transchegaraviylik; jinoiy yurisdiksiya.

**Annotatsiya:** Mazkur maqolada kiberjinoyatchilik tushunchasi va uning xalqaro huquqdagi ko‘p qatlamli kategoriya sifatidagi huquqiy mohiyati tadqiq etiladi. Tadqiqotning maqsadi – axborot-kommunikatsiya texnologiyalaridan foydalangan holda sodir etiladigan jinoyatlarga qarshi kurashda davlatlarning xalqaro hamkorligining definitsion poydevorini aniqlash hamda O‘zbekiston Respublikasi milliy qonunchiligini 2024-yilgi BMTning Kiberjinoyatchilikka qarshi konvensiyasi bilan uyg‘unlashtirish yo‘nalishlarini belgilashdan iborat. Tadqiqotning metodologik asosini tarixiy-huquqiy, qiyosiy-huquqiy, tizimli va formal-dogmatik usullar, shuningdek universal, mintaqaviy va integratsion darajadagi xalqaro shartnomalar tahlili tashkil etdi. «Kompyuter jinoyatchiligi – kiberjinoyatchilik – sun’iy intellektdan foydalangan holda sodir etiladigan huquqbuzarliklar» terminologik evolyutsiyasi xalqaro-huquqiy tartibga solish predmetining tajovuzlarning texnologik arxitekturasiga ergashib ketma-ket kengayib borishini aks ettirishi ko‘rsatib o‘tildi. Kiberjinoyatchilikning huquqiy mohiyati yagona definitsiya bilan emas, balki uch shartnomaviy qatlam – universal (2024-yilgi BMT Konvensiyasi), mintaqaviy (2001-yilgi Budapesht konvensiyasi) va integratsion (MDH va SHHT hujjatlari) – arxitekturasi bilan belgilanishi asoslandi; bu qatlamlarning umumiy belgisi tegishli qilmishlarning jinoyat deb e’tirof etilishi va xalqaro hamkorlikni obyektiv talab qilishidir. Kiberjinoyatchilik, kiberterrorizm va harbiy xarakterdagi

kiberoperatsiyalarni subyekt, maqsad va motiv, oqibatlarning xarakteri hamda qo‘llaniladigan huquqiy rejim bo‘yicha ajratish mezonlari taklif qilindi. O‘zbekiston Respublikasi milliy huquqi bilan universal standart o‘rtasidagi to‘rtta terminologik dissonans aniqlangan hamda respublika qonunchiligiga implementatsiya qilishga yaroqli kiberjinoyatchilikning xalqaro-huquqiy aspektdagi mualliflik ta’rifi ishlab chiqildi.

# КИБЕРПРЕСТУПНОСТЬ В МЕЖДУНАРОДНОМ ПРАВЕ: ПОНЯТИЕ И ПРАВОВАЯ ПРИРОДА

***Шухрат Атаханов***
*Независимый соискатель*

## О СТАТЬЕ

**Ключевые слова:** киберпреступность; преступления в сфере информационных технологий; Конвенция ООН против киберпреступности; Будапештская конвенция; международное сотрудничество; доказательства в электронной форме; информационная безопасность; Республика Узбекистан; трансграничность; уголовная юрисдикция.

**Аннотация:** В статье исследуются понятие и правовая природа киберпреступности как многоуровневой категории международного права. Цель исследования – выявить дефиниционный фундамент международного сотрудничества государств в борьбе с преступлениями, совершаемыми с использованием информационно-коммуникационных технологий, и определить направления гармонизации национального законодательства Республики Узбекистан с Конвенцией Организации Объединенных Наций против киберпреступности 2024 года. Методологическую основу работы составили историко-правовой, сравнительно-правовой, системный и формально-догматический методы, а также анализ международных договоров универсального, регионального и интеграционного уровней. Показано, что терминологическая эволюция «компьютерная преступность – киберпреступность – деяния с использованием искусственного интеллекта» отражает последовательное расширение предмета международно-правового регулирования вслед за технологической архитектурой

посягательств. Обосновывается тезис о том, что правовая природа киберпреступности определяется не единой дефиницией, которой сознательно избежали как Будапештская конвенция, так и Конвенция ООН, а архитектурой трех договорных слоев: универсального (Конвенция ООН 2024 г.), регионального (Будапештская конвенция 2001 г.) и интеграционного (акты СНГ и ШОС); общим знаменателем этих слоев является признание соответствующих деяний уголовно наказуемыми и объективно требующими международного сотрудничества. Предложены критерии демаркации киберпреступности, кибертерроризма и кибероперaций военного характера по субъекту, цели и мотиву, характеру последствий и применимому правовому режиму. Выявлены четыре терминологических диссонанса между национальным правом Республики Узбекистан и универсальным стандартом и сформулировано авторское определение киберпреступности в международно-правовом аспекте, пригодное для имплементации в законодательство Республики Узбекистан.

**Введение.** Стремительная цифровая трансформация государственного управления, экономики и общественных отношений неизбежно сопровождается ростом числа преступлений, совершаемых с использованием информационно-коммуникационных технологий (далее – ИКТ). Трансграничный характер таких деяний и формирование доказательств в электронной форме делают невозможным их эффективное предупреждение, раскрытие и расследование усилиями одного государства и предопределяют объективную потребность в международном сотрудничестве. Актуальность темы приобрела новое измерение после того, как 24 декабря 2024 г. Генеральная Ассамблея ООН резолюцией 79/243 приняла Конвенцию Организации Объединенных Наций против киберпреступности – первый универсальный международный договор в данной сфере, открытый для подписания на церемонии в Ханое 25–26 октября 2025 г.

Международное сотрудничество государств в борьбе с киберпреступностью строится на дефиниционном фундаменте: объем взаимных обязательств, пределы

уголовной юрисдикции и допустимость процессуальных действий на территории другого государства определяются тем, как договор и национальное законодательство очерчивают сам предмет борьбы. Между тем до принятия Конвенции ООН ни один универсальный международный договор не содержал сколько-нибудь завершенного понятийного аппарата в данной сфере. Сам процесс разработки Конвенции, инициированный резолюцией Генеральной Ассамблеи ООН от 27 декабря 2019 г. № 74/247 об учреждении специального межправительственного комитета экспертов открытого состава, продемонстрировал, что терминологическая децентрализация является не техническим дефектом правотворчества, а отражением принципиальных расхождений государств в понимании правовой природы посягательств, совершаемых с использованием ИКТ.

**Генезис и терминологическая эволюция понятия киберпреступности**

Первым законодательным опытом осмысления рассматриваемого круга деяний принято считать представленный в 1977 г. в Конгрессе США законопроект сенатора А. Рибикоффа (Federal Computer Systems Protection Act), который не был принят, однако задал исследовательскую и правотворческую повестку на последующие десятилетия. На этом этапе в научном обороте доминировала категория «компьютерная преступность», а преступление мыслилось преимущественно как локализованное деяние, совершаемое в отношении изолированной вычислительной системы или при ее посредстве. Второй этап эволюции связан с переходом от автономных вычислительных систем к сетевой архитектуре. Распространение сети Интернет ликвидировало территориальную привязку посягательства, что потребовало иной терминологической матрицы: категория «киберпреступность» стала отражать сетевую, трансграничную природу деяний. Кульминацией этапа стала Конвенция Совета Европы о киберпреступности (Будапешт, 23 ноября 2001 г., ETS № 185), которая, показательно, отказалась от легального определения киберпреступности, ограничившись перечнем криминализуемых деяний и процессуальных полномочий. В англоязычной доктрине этот период породил устойчивую трехчленную типологию, восходящую к Дж. Клафу: кибер-зависимые преступления, которые принципиально невозможны без ИКТ; кибер-ассоциированные – традиционные деяния, масштаб которых экспоненциально возрастает за счет сетевой среды; и деяния, в которых компьютер используется инструментально. Значение этой типологии для международного права состоит в том, что она продемонстрировала двусоставность предмета регулирования: договор должен одновременно охватывать и новые объекты правовой охраны (данные, системы, их целостность и доступность), и новые способы совершения давно известных преступлений.

Третий, формирующийся в настоящее время этап связан с появлением деяний, совершаемых с использованием систем искусственного интеллекта: автоматизированная генерация вредоносного кода, дипфейки как орудие мошенничества и дискредитации, автономные атакующие агенты. В евразийской правовой доктрине эта проблематика уже получила отражение: в частности, в сравнительном анализе уголовного законодательства Узбекистана и Казахстана обосновывается тезис о том, что действующие составы, построенные вокруг непосредственного человеческого действия, не в полной мере охватывают делегирование противоправного результата самообучающимся системам. Терминологическая эволюция свидетельствует, следовательно, не о смене модных слов, а о последовательном расширении предмета международно-правового регулирования вслед за технологической архитектурой посягательства.

Параллельно с эволюцией термина происходило доктринальное осмысление виртуального пространства как новой сферы международно-правового регулирования. В доктрине выделились два полюса. Первый, условно «либертарианско-юрисдикционный», исходит из презумпции минимального государственного вмешательства в глобальную сеть и из приоритета частноправовых и технических механизмов управления ею; второй, «суверенитарный», закрепленный прежде всего в правотворчестве евразийских интеграционных объединений, рассматривает информационное пространство как сферу осуществления государственного суверенитета. Показательно, что Соглашение между правительствами государств – членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности (Екатеринбург, 16 июня 2009 г.) оперирует не категорией «преступление», а каталогом угроз международной информационной безопасности, включая информационное оружие, информационную войну, информационный терроризм и информационную преступность. Как отмечал коллектив авторов под редакцией М.Б. Касеновой, расхождение базовых моделей – «борьба с киберпреступностью» как правоприменительная задача versus «обеспечение информационной безопасности» как задача суверенитета – десятилетиями блокировало формирование универсального договора. А.Г. Волеводз обосновывал, что выход из этого тупика лежит не через унификацию дефиниций, а через стандартизацию механизмов сотрудничества при сохранении национального усмотрения в вопросах криминализации. Именно этот подход в конечном счете и был реализован в архитектуре Конвенции ООН 2024 г.

**Доктринальные подходы к определению киберпреступности**

В национально юридической науке понятие преступлений в сфере информационных технологий разрабатывалось преимущественно в русле системного анализа Особенной части национального уголовного закона. М.Х. Рустамбаев, анализируя родовой и видовой объекты соответствующих составов, исходит из того, что посягательства в сфере информационных технологий образуют самостоятельную группу преступлений против общественной безопасности и общественного порядка, объединенных специфическим предметом – информацией, находящейся в информационно-вычислительных системах, сетях и их составных частях. Этот объектно-центричный подход, унаследованный от классической уголовно-правовой догматики, обеспечивает строгость квалификации, однако ограничивает предметное поле собственно «компьютерными» деяниями. Дополнительную, политико-правовую линию формируют исследования государственной политики противодействия цифровым преступлениям: Г.А. Саъдуллаев и Л.Э. Хамракулов, анализируя национальный опыт, связывают понятие киберпреступности не столько с предметом посягательства, сколько с угрозой информационной безопасности личности, общества и государства и указывают на институциональные факторы – дефицит кадров, сложность международного взаимодействия – как на элементы фактической характеристики данного вида преступности. Научная школа стран СНГ исторически сформировала международно-сотрудническую парадигму понятия. Фундаментальная монография А.Г. Волеводза 2002 г. впервые в постсоветской науке представила противодействие компьютерным преступлениям как комплексную проблему международного сотрудничества, объединив анализ национальных законодательств более чем 25 государств, документов ООН, Совета Европы, «Группы восьми» и СНГ с исследованием специфики следов компьютерных преступлений и доказывания в компьютерных сетях. В более поздней работе тот же автор закрепил термин «киберпреступность» в русскоязычном научном обороте и обосновал приоритет стандартизации процедур взаимодействия над унификацией материальных составов. Криминологическая рамка транснациональности восполнена в работах В.А. Номоконова, под редакцией которого транснациональная организованная преступность определена как явление, выходящее за пределы юрисдикции одного государства и требующее качественно иных, наднациональных по форме мер контроля. Применительно к киберпреступности эта рамка имеет прямое значение: трансграничность здесь не факультативный признак отдельных деяний, а имманентное свойство сетевой среды совершения.

Зарубежная доктрина представлена тремя исследовательскими направлениями. Первое – догматическое: Дж. Клаф, опираясь на законодательство Австралии, Канады,

Великобритании и США, вывел общие принципы уголовно-правовой охраны данных и систем и показал, что расхождения национальных составов носят не концептуальный, а преимущественно терминологический характер. Второе – институциональное: Ш. Шьольберг и С. Гернаути-Хели в экспертном докладе «Глобальный договор о кибербезопасности и киберпреступности» еще в 2011 г. обосновывали необходимость универсального договора под эгидой ООН, указывая на недопустимость ситуации, при которой единственным всеобъемлющим инструментом остается региональная конвенция. Третье – криминологическое: Р. Бродхерст в исследованиях глобального правоприменения и организационных форм киберпреступности доказал, что значительная часть деяний совершается структурированными группами с разделением труда, что стирает грань между «киберпреступностью» и транснациональной организованной преступностью и обусловливает востребованность механизмов Конвенции ООН против транснациональной организованной преступности 2000 г. в этой сфере.

**Разграничение киберпреступности и смежных категорий**

Для целей международного права принципиальна демаркация понятий «киберпреступность», «кибертерроризм» и «кибератака (кибервойна)», поскольку за каждой из них закреплен особый правовой режим. Киберпреступность подпадает под режим уголовно-правового сотрудничества (правовая помощь, выдача, обмен электронными доказательствами) независимо от мотива деятеля. Кибертерроризм, как показал Ш. Шьольберг в специальном исследовании соотношения реальности и мифологизации этой угрозы, отграничивается не способом, а субъективной стороной и целью: политически мотивированное запугивание населения или принуждение властей посредством разрушительного воздействия на информационные системы; соответствующие деяния втягиваются в режим универсальных антитеррористических конвенций. Наконец, кибероперации, достигающие по масштабу и последствиям уровня применения силы, относятся к сфере jus ad bellum и международного гуманитарного права, что детально обосновано в Таллиннском руководстве 2.0 о применимом к кибероперациям международном праве. Евразийская договорная практика воспроизводит ту же триаду в терминах «информационная преступность – информационный терроризм – информационная война», закрепленных в качестве самостоятельных угроз в приложении к Соглашению ШОС 2009 г.. Следовательно, киберпреступность занимает в этой системе центральное, но строго очерченное место: ее правовой режим – режим уголовной юстиции, а не режим безопасности или военного права, и любое расширительное толкование понятия (например, включение в него политически мотивированного контента) размывает

договорные механизмы сотрудничества, что подтвердила и переговорная история Конвенции ООН 2024 г.

**Понятийный аппарат конвенции ООН против киберпреступности 2024 г. в системе международно-договорных режимов**

Принятие Конвенции ООН против киберпреступности завершило пятилетний переговорный цикл, начатый резолюцией 74/247 (2019 г.) и продолженный резолюцией 75/282 (2021 г.), определившей регламент Специального комитета. Конвенция включает 68 статей, сгруппированных в девять глав, и четыре приложения с толкованиями отдельных положений. Ее понятийный вклад принципиален по трем направлениям. Во-первых, статья 2 впервые на универсальном уровне закрепляет операциональные дефиниции: «информационно-коммуникационная система», «электронные данные», «трафик-данные», «контентные данные», «провайдер услуг», «личные данные», а также «серьезное преступление» – деяние, наказуемое лишением свободы на срок не менее четырех лет или более строгим наказанием, – выполняющее роль критерия для расширенного обмена электронными доказательствами. Во-вторых, глава II (статьи 7–21) формирует универсальное ядро криминализации: неправомерный доступ, неправомерный перехват, вмешательство в отношении электронных данных и информационно-коммуникационных систем, злоупотребление устройствами, подделка, хищение и мошенничество, связанные с такими системами, правонарушения против детей в сетевой среде и несанкционированное распространение интимных изображений. В-третьих, Конвенция создает первый глобальный режим сбора и обмена доказательствами в электронной форме применительно к любым серьезным преступлениям, а также круглосуточную сеть оперативного взаимодействия.

25–26 октября 2025 г. в Ханое (Вьетнам) состоялась церемония подписания Конвенции: в первый день ее подписали 65 государств, всего в церемонии участвовали делегаты более чем 100 стран. Республика Узбекистан, принимавшая активное участие в разработке и согласовании проекта на всех этапах переговорного процесса, подписала Конвенцию; документ от имени Правительства Республики Узбекистан подписал спикер Законодательной палаты Олий Мажлиса Н. Исмаилов. Конвенция вступит в силу по истечении 90 дней после депозитирования сороковой ратификационной грамоты, что открывает для Узбекистана период приведения национального законодательства в соответствие с ее положениями. Показательно, что Конвенция, подобно Будапештской, не дает легального определения киберпреступности: универсальный понятийный аппарат сформирован не через дефиницию родового понятия, а через согласованный перечень

деяний и дефиниции технических терминов – цена, которую государства заплатили за достижение глобального консенсуса.

Сравнительный анализ с предшествующими режимами позволяет уточнить правовую природу нового универсального стандарта. Будапештская конвенция 2001 г., действующая с 1 июля 2004 г. и объединяющая ныне более 75 государств-участников, исторически выполняла роль модельного стандарта: она впервые синхронизировала перечень составов (статьи 2–11) с процессуальными полномочиями по сохранению и раскрытию компьютерных данных. Ее ограничение состоит не в качестве норм, а в генезисе: будучи региональным инструментом Совета Европы, она воспринимается значительной частью государств – в том числе странами Евразии – как внешне навязанный стандарт; особую критику вызывала статья 32(b), допускающая трансграничный доступ к общедоступным данным без дополнительного разрешения. Модель СНГ, напротив, строилась вокруг легальных дефиниций: Соглашение о сотрудничестве государств – участников СНГ в борьбе с преступлениями в сфере компьютерной информации (Минск, 1 июня 2001 г.) определило соответствующее преступление как уголовно наказуемое деяние, предметом посягательства которого является компьютерная информация. В развитие этой линии Соглашение о сотрудничестве государств – участников СНГ в борьбе с преступлениями в сфере информационных технологий (Душанбе, 28 сентября 2018 г., вступило в силу 12 марта 2020 г.), подписанное в том числе Президентом Республики Узбекистан, обновило понятийный ряд («компьютерная система», «компьютерная информация», «несанкционированный доступ к информации», «вредоносная программа») и расширило формы практического взаимодействия правоохранительных органов. Стратегия обеспечения информационной безопасности государств – участников СНГ 2019 г. дополнила эту систему дефиницией информационной преступности как использования информационных ресурсов и (или) воздействия на них в информационном пространстве в противоправных целях. Модель ШОС, как показано выше, уголовно-правовую дефиницию подменяет каталогом угроз международной информационной безопасности. Конвенция ООН 2024 г. синтезирует достоинства этих подходов: от Будапештской конвенции она заимствовала структуру «криминализация – процессуальные полномочия – международное сотрудничество», от евразийской практики – уважение к суверенитету и отказ от автоматического трансграничного доступа к данным, от модели СНГ – внимание к согласованию терминов.

**Заключение.** Проведенное исследование позволяет сформулировать следующие выводы.

Во-первых, киберпреступность в международном праве сложилась как многоуровневая категория, правовая природа которой определяется не единой дефиницией (ее сознательно избежали и Будапештская конвенция, и Конвенция ООН 2024 г.), а архитектурой трех договорных слоев: универсального, деяние-центричного и правозащитно ориентированного (Конвенция ООН 2024 г.); регионального модельного, правоприменительно-центричного (Будапештская конвенция 2001 г.); и интеграционного, безопасностно-центричного (акты СНГ и ШОС). Общим знаменателем всех трех слоев является признание соответствующих деяний уголовно наказуемыми и объективно требующими международного сотрудничества; различия касаются предметного охвата и баланса между задачами уголовной юстиции и задачами информационной безопасности.

Во-вторых, юридическая демаркация киберпреступности, кибертерроризма и кибероперациий военного характера должна проводиться по четырем критериям: субъект деяния; его цель и мотив; характер и масштаб последствий; применимый правовой режим (уголовно-правовое сотрудничество – универсальные антитеррористические конвенции – jus ad bellum и международное гуманитарное право). Смешение этих категорий разрушает договорные механизмы правовой помощи, поскольку каждый режим имеет собственные основания отказа, политические исключения и процессуальные гарантии.

В-третьих, Республика Узбекистан сформировала двухконтурную национальную систему регулирования: стратегический контур (Стратегия «Цифровой Узбекистан – 2030», Закон № ЗРУ-764, постановление № ПП-167) и уголовно-правовой контур (глава XX[1] УК РУз), в целом соответствующую евразийской модели, однако нуждающуюся в гармонизации с Конвенцией ООН 2024 г. по четырем направлениям: закрепление термина «киберпреступность»; введение категорий «электронные данные», «трафик-данные» и «контентные данные»; восполнение пробелов в криминализации кибер-ассоциированных деяний; детализация режима доказательств в электронной форме при трансграничном обмене. Подписание Конвенции в Ханое 25–26 октября 2025 г. открывает для республики период приведения законодательства в соответствие с универсальным стандартом, и от качества этой имплементации будет зависеть практическая работоспособность механизмов международного сотрудничества в борьбе с киберпреступностью.

В-четвертых, системообразующими квалифицирующими признаками киберпреступности в международно-правовом аспекте являются: а) совершение деяния посредством информационно-коммуникационных систем либо направленность деяния против безопасности таких систем и обрабатываемых ими данных; б) уголовная наказуемость по национальному праву на основе договорно согласованного минимума; в)

трансграничность как типичный, хотя и не обязательный, признак; г) образование доказательств в электронной форме, предопределяющее объективную невозможность эффективного расследования без международного процессуального сотрудничества.

С учетом изложенного представляется возможным предложить следующее авторское определение, пригодное для последующей имплементации в законодательство Республики Узбекистан: киберпреступность в международно-правовом аспекте – это совокупность предусмотренных международными договорами и национальным уголовным законодательством умышленных общественно опасных деяний, совершаемых посредством информационно-коммуникационных систем либо направленных против целостности, доступности и конфиденциальности электронных данных и таких систем, которые, как правило, носят трансграничный характер, образуют доказательства в электронной форме и в силу указанных свойств не могут быть эффективно предупреждены, раскрыты и расследованы без международного сотрудничества государств. Предложенная дефиниция совместима со статьей 2 Конвенции ООН 2024 г., поглощает предметный состав главы XX[1] УК РУз и одновременно охватывает кибер-ассоциированные деяния, что устраняет выявленные выше терминологические диссонансы.

**Список использованной литературы:**

1. Закон Республики Узбекистан от 15.04.2022 № ЗРУ-764 «О кибербезопасности» // Национальная база данных законодательства Республики Узбекистан, 16.04.2022. URL: https://lex.uz.

2. Постановление Президента Республики Узбекистан от 31.05.2023 № ПП-167 «О дополнительных мерах по совершенствованию системы обеспечения кибербезопасности объектов критической информационной инфраструктуры Республики Узбекистан» // Национальная база данных законодательства Республики Узбекистан, 02.06.2023, № 07/23/167/0321.

3. Уголовный кодекс Республики Узбекистан (принят 22.09.1994, введен в действие с 01.04.1995, с последующими изменениями и дополнениями) // Национальная база данных законодательства Республики Узбекистан. URL: https://lex.uz/docs/111457 .

4. Указ Президента Республики Узбекистан от 05.10.2020 № УП-6079 «Об утверждении Стратегии «Цифровой Узбекистан – 2030» и мерах по ее эффективной реализации» // Национальная база данных законодательства Республики Узбекистан. URL: https://lex.uz/docs/5031048.

5. Конвенция о киберпреступности (ETS № 185; Будапешт, 23.11.2001; вступила в силу 01.07.2004) // Council of Europe Treaty Office. URL: https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=185.

6. 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 (принята резолюцией Генеральной Ассамблеи ООН от 24.12.2024 № 79/243) // Официальные документы ООН. URL: https://docs.un.org/ru/A/RES/79/243.

7. Резолюция Генеральной Ассамблеи ООН от 26.05.2021 № 75/282 «Специальный комитет по разработке всеобъемлющей международной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях» // Официальные документы ООН. URL: https://docs.un.org/ru/A/RES/75/282.

8. Резолюция Генеральной Ассамблеи ООН от 27.12.2019 № 74/247 «Противодействие использованию информационно-коммуникационных технологий в преступных целях» // Официальные документы ООН. URL: https://docs.un.org/ru/A/RES/74/247 .

9. Соглашение между правительствами государств – членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности (Екатеринбург, 16.06.2009) // Бюллетень международных договоров. 2012. № 1. С. 13–21.

10. Соглашение о сотрудничестве государств – участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации (Минск, 01.06.2001) // СПС «Гарант». URL: https://base.garant.ru/12123778/.

11. Соглашение о сотрудничестве государств – участников Содружества Независимых Государств в борьбе с преступлениями в сфере информационных технологий (Душанбе, 28.09.2018; вступило в силу 12.03.2020) // СПС «Гарант». URL: https://base.garant.ru/72087644/.

12. Стратегия обеспечения информационной безопасности государств – участников Содружества Независимых Государств (утв. Решением Совета глав правительств СНГ от 25.10.2019, г. Москва) // Совет глав правительств СНГ. URL: http://www.intermedia.ru/uploads/72b6a0.pdf.

13. Вехов В.Б. Компьютерные преступления: способы совершения и раскрытия: учеб.-практ. пособие / под ред. Б.П. Смагоринского. М.: Право и закон, 1996. 182 с.

14. Волеводз А.Г. Противодействие компьютерным преступлениям: правовые основы международного сотрудничества. М.: Юрлитинформ, 2002. 496 с.

15. Волеводз А.Г. Противодействие киберпреступности: правовые основы международного сотрудничества. М.: Юрлитинформ, 2014. 352 с.

16. Рустамбаев М.Х. Курс уголовного права Республики Узбекистан. Особенная часть: учебник для вузов. 2-е изд., доп. и перераб. Ташкент: Военно-технический институт Национальной гвардии Республики Узбекистан, 2018. Т. 3: Преступления против личности, мира и безопасности. 423 с.

17. Транснациональная организованная преступность: дефиниции и реальность: монография / отв. ред. В.А. Номоконов. Владивосток: Изд-во Дальневосточного университета, 2001.

18. Clough J. Principles of Cybercrime. 2nd ed. Cambridge: Cambridge University Press, 2015. 524 p.

19. Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations / ed. by M.N. Schmitt. 2nd ed. Cambridge: Cambridge University Press, 2017.

20. Волчинская Е.К., Грицай Г.А., Дембоски Л., Демидов О.В., Зинина У.В., Касенова М.Б. и др. Управление интернетом и борьба с киберпреступностью: глобальные угрозы и российские интересы // Индекс безопасности. 2013. Т. 19. № 4 (107). С. 89–106.

21. Саъдуллаев Г.А., Хамракулов Л.Э. Государственная политика Республики Узбекистан в области противодействия преступлениям в сфере цифровых технологий и безопасности // Eurasian Journal of Academic Research. 2024. DOI: 10.5281/zenodo.11399956.

22. Фазилов Ф.М., Аманжолова Б.А. Искусственный интеллект и уголовное право в Узбекистане и Казахстане // Universum: экономика и юриспруденция: электрон. науч. журн. 2025. URL: https://cyberleninka.ru/article/n/iskusstvennyy-intellekt-i-ugolovnoe-pravo-v-uzbekistane-i-kazahstane.

23. Broadhurst R. Developments in the Global Law Enforcement of Cyber-crime // Policing: An International Journal of Police Strategies & Management. 2006. Vol. 29. № 3. P. 408–433.

24. Broadhurst R., Grabosky P., Alazab M., Bouhours B., Chon S. Organizations and Cyber Crime: An Analysis of the Nature of Groups Engaged in Cyber Crime // International Journal of Cyber Criminology. 2014. Vol. 8. № 1. P. 1–20.

25. Делегация Узбекистана приняла участие в подписании Конвенции ООН против киберпреступности // ИА «Дунё». 27.10.2025. URL: https://dunyo.info.

26. Конвенция ООН против киберпреступности открылась для подписания в Ханое, Вьетнам // Управление ООН по наркотикам и преступности. 25.10.2025. URL: https://www.unodc.org/unodc/ru/press/releases/2025/October/un-convention-against-cybercrime-opens-for-signature-in-hanoi--viet-nam.html.

27. Шестьдесят пять стран подписали Конвенцию ООН против киберпреступности // Служба новостей ООН. 25.10.2025. URL: https://news.un.org/ru/story/2025/10/1466671.

28. Schjolberg S. Terrorism in Cyberspace – Myth or Reality? (2007) // Cybercrime Law. URL: http://www.cybercrimelaw.net/documents/Terrorism_in_cyberspace.pdf.

29. Schjolberg S. The History of Global Harmonization on Cybercrime Legislation – The Road to Geneva (2008) // Cybercrime Law. URL: http://www.cybercrimelaw.net.

30. Schjolberg S., Ghernaouti-Helie S. A Global Treaty on Cybersecurity and Cybercrime. 2nd ed. (2011) // Cybercrime Law. URL: http://www.cybercrimelaw.net.

31. The Criminal Code of the Republic of Uzbekistan. Chapter XX-1. Articles 278-1 – 278-6 // UNODC SHERLOC. URL: https://www.unodc.org/cld/es/legislation/uzb/the_criminal_code_of_the_republic_of_uzbekistan_russian/chapter_xx-1/articles_278-1_-_278-6/chapter_xx-1.html.