Исхакова Лавиза Фуатовна
Ўзбекистон Республикаси Давлат ва ҳуқуқ институти етакчи илмий ходими. ю.ф.н., доцент

АХБОРОТ ХАВФСИЗЛИГИ ВА КИБЕРЖИНОЯТЧИЛИККА ҚАРШИ КУРАШИШ СОҲАСИДАГИ ХАЛҚАРО ҲУҚУҚИЙ ҲУЖЖАТЛАРНИ КЎРИБ ЧИҚИШ: ҲОЗИРГИ ҲОЛАТ ВА ҚУТҚУЛАР

Исхакова Лавиза Фуатовна
Доктор юридических наук, доцент, ведущий научный сотрудник Института государства и права Республики Узбекистан,

ОБЗОР МЕЖДУНАРОДНО-ПРАВОВЫХ ДОКУМЕНТОВ В СФЕРЕ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ПРОТИВОДЕЙСТВИЯ КИБЕРПРЕСТУПНОСТИ: СОВРЕМЕННОЕ СОСТОЯНИЕ И ВЫЗОВЫ

Iskhakova Laviza
Leading Researcher of the Institute of State and Law of the Republic of Uzbekistan, Ph.D. Assoicate Professor

REVIEW OF INTERNATIONAL LEGAL DOCUMENTS IN THE FIELD OF INFORMATION SECURITY AND COUNTERING CYBERCRIME: CURRENT STATE AND CHALLENGES

Аннотация. *Мақола ахборот хавфсизлиги ва кибержиноятчиликка қарши курашиш соҳасидаги халқаро ҳуқуқий ҳужжатлар таҳлилини ўз ичига олади. БМТ, ХЕИ, Европа Иттифоқи, ОЕСД, МДҲ, ШҲТ ҳужжатлари таҳлил қилинади. Ўзбекистон Республикасининг ушбу ҳужжатларга муносабати, шунингдек, халқаро ҳуқуқий тартибга солишни талаб этувчи муаммолар кўрсатилган.*

Аннотация. *Статья содержит обзор международно-правовых документов в сфере обеспечения информационной безопасности и противодействия киберпреступности. Анализируются документы ООН, МСЭ, ЕС, ОЭСР, СНГ, ШОС. Представлена позиция Узбекистана по отношению к этим документам, а также проблемы, требующие международно-правового регулирования.*

Annotation. *The article contains an overview of international legal documents in the field of information security and combating cybercrime. Documents of the UN, ITU, EU, OECD, CIS, SCO are analyzed. The position of Uzbekistan in relation to these documents, as well as problems requiring international legal regulation are presented.*

Введение

Узбекистан планомерно и неуклонно движется к информационному обществу. Ставка сделана на цифровизацию и телекоммуникацию как базовые технологии, обеспечивающие интеграцию республики в международное информационное общество.

Высокие технологие проникли во все сферы жизни общества, от образования до промышленности, от управления до государственных услуг, что приводит к трансформации практически всех государственно-правовых явлений.

Логика регулирования общественных отношений в сфере информационных технологий объективно находится в плоскости как национального, так и международного права. Цифровые технологии преобразовали систему человеческих коммуникаций и взаимодействий. Любая сфера деятельности в масштабе индивида, группы или общества в целом связана с ИКТ, трансформируется за счет них или опосредуется ими. И международные отношения не являются исключением.

Настоящая статья обобщает и систематизирует документы, разработанные за последние годы на международно-правовом уровне различными международными организациями. Кроме того, следует четко определить объект и круг этих документов, подлежащих анализу – документы, относящиеся к правовому обеспечению информационной безопасности.

Проблемой является интерпретация и понимание самого термина «информационная безопасность» или «кибербезопасность», которое в одних случаях воспринимаются как идентичные понятия, а в других понимаются по-разному. А в документах МСЭ используется словосочетание «доверие и безопасность при использовании ИКТ».

В последние годы практически во всех странах и международных организациях уделяется внимание проблемам цифровизации. Анализ этих актов создает достаточно целостную картину, отражающую мировые процессы.

Международные организации и их документы

Международные организации, такие как ООН, МСЭ, ЮНЕСКО, Совет Европы, ОЭСР уделяют особое внимание в своих документах вопросам информационной безопасности. В этом контексте можно упомянуть прежде всего такие резолюции ГА ООН, как Резолюция 68/198 ГА ООН от 20 декабря 2013 года об использовании информационно-коммуникационных

технологий (ИКТ) в целях развития[1]; Резолюция 71/199 ГА ООН от 19 декабря 2016 года о праве на неприкосновенность личной жизни в цифровой век[2], Резолюция 68/243 ГА ООН от 27 декабря 2013 года о достижениях в сфере информатизации и телекоммуникаций в контексте международной безопасности[3], Резолюция 57/239 ГА ООН от 20 декабря 2002 года о создании глобальной культуры кибербезопасности, Резолюция 56/121 ГА ООН от 23 января 2002 года о борьбе с преступным использованием информационных технологий [4], Резолюция 55/63 ГА ООН от 22 января 2001 года о борьбе с преступным использованием информационных технологий [5].

В международных документах подчеркивается, что для большинства стран, вовлеченных в информационное общество, возрастает значение кибербезопасности. Следует обратить внимание на то, что в международных документах информационная безопасность и кибербезопасность используются как равнозначные термины. Резолюция 57/239 ГА ООН определяет глобальную культуру кибербезопасности как сложное понятие, включающее в себя девять элементов: (1) осведомленность, (2) ответственность, (3) реагирование, (4) этика, (5) демократия, (6) оценка риска, (7) проектирование и внедрение средств обеспечения безопасности, (8) управление обеспечением безопасности, (9) переоценка.

Концепция культуры кибербезопасности в этих документах рассматривается как непрерывный и интеграционный процесс, основанный на руководящих указаниях и рекомендациях, которые международное сообщество решит применять в целях расширения своих возможностей по борьбе с киберугрозами и атаками, включая динамичный, интеграционный, основанный на оценке рисков подход, отражающий постоянно меняющийся характер угроз и уязвимостей, и необходимость международного сотрудничества [6].

Вопросы безопасности выделены отдельным направлением в документах Женевского и Тунисского саммитов по управлению информационным обществом. Так направление С5 Женевских принципов формулируется как «Укрепление доверия и безопасности при использовании ИКТ» и включает в себя содействие международному сотрудничеству для повышения надежности и защиты целостности как данных, так и сетей, анализа существующих и потенциальных угроз в области ИКТ; предупреждение, обнаружение проявления киберпреступности и ненадлежащего использования ИКТ и реагирование на эти проявления; усиление на международном уровне институциональной поддержки профилактики таких инцидентов и ликвидации их последствий; содействие образованию и повышению осведомленности.

Анализ содержания этих резолюций показывает, что они являются своеобразными руководящими документами для каждого государства, для выработки и функционирования собственных систем информационной безопасности.

В Тунисских обязательствах выделяется роль государства в обеспечении и формировании культуры кибербезопасности, которая требует действий на национальном уровне с целью укрепления безопасности при обеспечении защиты информации личного характера, неприкосновенности частной жизни и данных. В этих обязательствах подчеркивается важность безопасного, непрерывного и стабильного функционирования Интернет и необходимость защиты его и других сетей ИКТ от возможного неблагоприятного воздействия или подверженности рискам. Для достижения целей развития, как указано в этом документе, ключевое значение имеет развитие инфраструктуры, создание человеческого потенциала, информационная безопасность и безопасность сетей.

МСЭ в рамках деятельности двух секторов стандартизации и развития (МСЭ-Т и МСЭ-D) анализирует вопросы и разрабатывает рекомендации и стандарты, относящиеся к укреплению доверия и безопасности при использовании ИКТ, включая стабильность и меры по противодействию спаму, вредоносным программным средствам, защите персональных данных и неприкосновенности частной жизни. МСЭ как специализированное учреждение ООН в сфере разработки международных рекомендаций и стандартов развития телекоммуникаций содействует достижению общего понимания среди правительств в вопросах укрепления доверия и безопасности при использовании ИКТ на национальном, региональном и международном уровнях. В документах этой организации разделяются сферы, которым следует заниматься МСЭ, сосредоточив ресурсы и программы на тех международных областях кибербезопасности, которые соответствуют ее основному мандату и опыту в технической сфере, от областей, относящихся к применению государствами правовых или политических принципов, связанных с национальной обороной, национальной безопасностью, контентом и киберпреступностью, находящихся в юрисдикции самого государства.

С помощью своих исследовательских комиссий МСЭ поддерживает разработку инфраструктуры, которая является основой происходящей цифровой трансформации мировой экономики, укрепляя доверие и безопасность при использовании ИКТ, в частности, при решении вопросов, связанных с существующими и будущими угрозами. МСЭ в области кибербезопасности предложил введение Глобального индекса кибербезопасности (GCI) с тем, чтобы содействовать осуществлению государственных стратегий и обмену информацией о деятельности, проводимой в отраслях и секторах.

В соответствии с Глобальным индексом кибербезопасности 2020 (Global Cybersecurity Index 2020) Узбекистан занял 70-е место среди 181 стран. На первом и втором местах находятся США, Великобритания, Саудовская Аравия, Эстония [7]. Глобальный индекс состоит из следующих компонентов: законодательные меры; технические меры; организационные меры; меры усиления потенциала; меры сотрудничества.

В данной сфере имеются примеры действующих международно-правовых актов, принятых на региональном уровне. Наиболее известными из них являются принятые в рамках Совета Европы Конвенция о защите частных лиц в отношении автоматизированной обработки данных личного характера от 28 января 1981 года[8] и Дополнительный протокол к ней, касающийся наблюдательных органов и трансграничной передачи данных от 8 ноября 2001 года [9], которые устанавливают обязательства государств по защите персональных данных при их автоматизированной обработке, трансграничной передаче, а также права субъектов персональных данных, которые должны быть обеспечены государствами. Представляется, что указанные документы могли бы стать основой для разработки и принятия соответствующих международно-правовых актов как в рамках ООН, так и в формате региональных международных организаций.

В настоящее время наиболее авторитетным международно-правовым актом комплексного характера является Конвенция Совета Европы о компьютерных преступлениях от 23 ноября 2001 года [10], участниками которой выступают 35 государств. 28 января 2003 г. также был принят Дополнительный протокол к Конвенции о преступлениях в сфере компьютерной информации, об инкриминировании расистских актов и совершенного ксенофоба при помощи информационных систем от 28 января 2003 года [11]. Данные акты определяют составы киберпреступлений, процессуальные аспекты борьбы с ними, устанавливают правила установления юрисдикции, а также регламентируют международное сотрудничество в борьбе с киберпреступностью.

Кроме того, в Европейском союзе уделяет особое внимание правам человека и защите персональных данных. Среди них можно отметить документы Европейского парламента и Совета Европы, принятые еще в 1997 году- Директиву 97/66/ ЕС, касающуюся процедур персональных данных и защиты частной жизни в секторе телекоммуникаций. (Directive 97/66/EC of European Parliament and of the Council of 15 December 1997 concerning the processing of person data and the protection of privecy in telecommunication sector).

В рамках ОЭСР можно отметить Канкунскую декларацию 2016 года о цифровой экономике: инновации рост и социальное благополучие, согласно которой государства-участники стремятся обеспечить свободный

оборот информации, сочетая открытость интернета и информационную безопасность, при условии защиты персональных данных и частной жизни. Или Рекомендации Совета ОЭСР по принципам разработки государственной политики в сфере интернета, Инструментарий цифрового правительства 2016 года, в котором выделены 12 принципов внедрения стратегий цифрового правительства и обеспечения информационной безопасности.

Генеральной Ассамблеей и иными органами ООН в последние годы уделялось повышенное внимание данной проблематике. Однако пристальное внимание к этим вопросам пока не повлекло принятие универсальных международных договоров, аналогичных названным документам Совета Европы. Между тем, наличие потребности в них признается международными экспертами. В частности, в рабочем документе, подготовленном Секретариатом Двенадцатого Конгресса ООН по предупреждению преступности и уголовному правосудию, прошедшего в Салвадоре (Бразилия) 12–19 апреля 2010 г. содержалась рекомендация о разработке глобальной конвенции против киберпреступности.

Характеризуя региональный уровень международного сотрудничества в рассматриваемой сфере, следует отметить, что в рамках СНГ действует Соглашение о сотрудничестве государств – участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации от 28 сентября 2018 года (вступил в силу для Республики Узбекистан 12 марта 2020 года) [12], которое отражает последние тенденции в использовании научно-технических достижений правонарушителями, и сотрудничество компетентных органов, ведущих борьбу с киберпреступностью. Оно регламентирует составы преступлений в сфере компьютерной информации, формы и содержание сотрудничества государств – участников СНГ в данной сфере, процедуру направления и исполнения запросов об оказании содействия в рамках Соглашения. Недостатком данного акта является узость его регулирования предмета, поскольку преступления в сфере компьютерной информации являются лишь одной из составляющих киберпреступности.

Институционализация киберпреступности как целостного и самостоятельного направления борьбы с преступностью представляется исключительно важной для организации успешного взаимодействия государств-участников СНГ. В этой связи необходимо принять соответствующих региональных международно-правовых актов в области противодействия киберпреступности в рамках СНГ, ШОС.

В рамках работы Межпарламентской Ассамблеи СНГ 28 ноября 2014 года приняты модельные законы: модельный закон СНГ «Об информации, информатизации и обеспечении информационной безопасности» и модельный закон «О критически важных объектах информационно-коммуникационной инфраструктуры».

Решением Совета глав правительств СНГ 28 октября 2016 года утверждена Стратегия сотрудничества государств – участников СНГ в построении и развитии информационного общества на период до 2025 года и План действий по ее реализации [13].

Одно из первых международных соглашений в области обеспечения международной информационной безопасности было подписано 16 июня 2009 года в Екатеринбурге правительствами государств – членов Шанхайской организации сотрудничества – Соглашение о сотрудничестве в области обеспечения международной информационной безопасности [14].

В Соглашении уделяется внимание на их деятельность, которая должна способствовать социальному и экономическому развитию и быть совместимой с задачами поддержания международной безопасности и стабильности. Деятельность Шанхайской организации сотрудничества должна соответствовать общепризнанным принципам и нормам международного права, включая принципы мирного урегулирования споров и конфликтов, неприменения силы, невмешательства во внутренние дела, уважения прав и основных свобод человека, а также принципам регионального сотрудничества и невмешательства в информационные ресурсы государств сторон.

Позиция Узбекистана

Узбекистан криминализировал деяния по киберпреступности в своем уголовном законодательстве, однако на уровне двухсторонних международных соглашений не решены вопросы международного расследования и уголовного преследования киберпреступности. В Уголовном кодексе Республики Узбекистан есть отдельная глава криминализующая киберпреступность.

Узбекистан поддерживает важность борьбы против терроризма во всех его формах и проявлениях в Интернете наряду с соблюдением прав человека и в соответствии с другими обязательствами по международному праву.

Правовую основу безопасности при использовании ИКТ в Республике Узбекистан составляют Законы РУ «О принципах и гарантиях свободы информации», «Об электронной цифровой подписи», «Об информатизации», «О защите персональных данных».

В целях реализации единой государственной политики в сфере информационной безопасности принято Постановление Президента Республики Узбекистан от 21 ноября 2018 года № ПП–4024 «О мерах по совершенствованию системы контроля за внедрением информационных технологий и коммуникаций, организации их защиты», которое определило основные задачи в сфере информационной безопасности:

– сбор, анализ и накопление данных о современных угрозах информационной безопасности, выработку рекомендаций и предложений по оперативному принятию эффективных организационных и

программно-технических решений, обеспечивающих предотвращение актов незаконного проникновения в информационные системы, ресурсы и базы данных государственных органов и организаций;

– взаимодействие с операторами и провайдерами сетей телекоммуникаций, правоохранительными органами в рамках проведения анализа, идентификации нарушителей, методов и средств, используемых при осуществлении несанкционированных либо деструктивных действий в информационном пространстве;

– проведение аттестации, экспертизы и сертификации аппаратных средств и программных продуктов, информационно-коммуникационных технологий, телекоммуникационного оборудования и иных технических средств на объектах информатизации (за исключением государственных секретов);

– оказание содействия в разработке и реализации политики информационной безопасности информационных систем и ресурсов государственных органов и организаций;

– выработку предложений по совершенствованию нормативно-правовой базы в сфере обеспечения информационной безопасности государственных информационных систем и ресурсов, а также национального сегмента сети Интернет;

– своевременное оповещение национальных пользователей сети Интернет о возникающих угрозах информационной безопасности в национальном сегменте сети Интернет, а также оказание консультационных услуг по защите информации [15].

Проблемы, требующие международно-правового регулирования

Анализ международных документов и стандартов в этой сфере важен не сам по себе, а с точки зрения поиска и определения различных моделей правовых режимов, обеспечивающих информационную безопасность страны в долгосрочной перспективе.

Традиционная иерархическая система правового регулирования не работает в отношении информационной безопасности из-за следующих обстоятельств:

– современное информационное пространство не ограничивается государственными границами;

– на международном уровне происходит смена парадигмы взаимодействия субъектов международного права при формировании права межгосударственных союзов и структур. В реальности круг субъектов стал шире и разнообразнее за счет участия в этих союзах ТНК, научных сообществ, международных СМИ и НПО;

– кроме того, усложнение цифровых технологий, киберфизических систем, порождаемых активным развитием искусственного интеллекта, требует поиска таких моделей правового регулирования, которые бы сочетали правовые, технические, моральные и корпоративные нормы.

Среди наиболее значимых проблем и вопросов, на которые необходимо найти ответы в международно-правовых документах:

– статус информации в публичных правоотношениях;

– критерии выработки государственной политики в информационной сфере;

– обеспечение прав граждан на доступ к информации и криминализация распространения цифровых данных;

– вопросы юридической ответственности, государственного суверенитета и юрисдикции в эпоху глобальной экономики;

– проблемы формирования системы международной информационной безопасности;

– противодействие киберпреступности и международное сотрудничество в этой сфере;

– под влиянием ИКТ и цифровизации даже вопросы международной безопасности приобретают иной оттенок. Масштаб и уровень деструктивного использования ИКТ неуклонно растет, а отсутствие необходимой международно-правовой базы, регулирующей деятельность государств в этой сфере, осложняет ситуацию.

В рамках международных организаций ведется активная дискуссия о том, кто должен управлять интернетом: эффективные стейкхолдеры (Stakeholders), корпорация ICANN, Международный союз электросвязи (МСЭ), Китай или другие государства. Сегодня регулирование отношений, связанных с интернетом, его управлением и безопасностью, закреплены в различных законодательных актах, резолюциях международных организаций, неформальных инициативах, правительственных и общественных проектах и актах в сфере информационной безопасности и управления интернетом.

Интернет на доктринальном и правоприменительном уровне рассматривается как:

А) техническое изобретение и Б) доступ к информации т.е. использование информации и как информационная услуга.

Это разграничение позволяет понять суть управления интернетом, с одной стороны, как управление многоуровневым процессом технической координации инфраструктуры интернета (IP-адреса, система доменных имен, корневые серверы, стандарты, протоколы) и, с другой – иные измерения управления интернетом: политические, социальные, экономические, этические, правовые.

Управление интернетом сформировалось и исторически сложилось как многосторонняя модель, основанная на саморегулировании, многостороннем партнерстве, включающем в себя все заинтересованные стороны: частный сектор, гражданское общество, бизнес, техническое и академическое сообщество, правительства и международные организации. Такая многосторонняя модель оказалась эффективной для обеспечения

стабильности, безопасности и доступности трансграничной инфраструктуры интернета. Управление интернетом связано с государствами как субъектами международного права. Вместе с тем, организационно-техническое функционирование интернета не связано с государством и его никто не может выключить. Однако технологические компоненты интернета подпадают под многочисленные государственные и национальные юрисдикции и государство может ввести ограничение на передачу информации, что является суверенным правом государства. Кроме того, государствам принадлежит ведущая роль в определении политики в сфере интернета и в формировании международно-правовой модели управления интернетом. Именно многосторонняя модель дала возможность создания устойчивого управления интернетом за более чем 50-летнюю историю своего существования.

Выводы и рекомендации

- Международные документы являются руководящими для каждого государства при выработке и функционировании национальных систем информационной безопасности.
- 1. Остро стоит вопрос единообразия и соответствия терминологии информационной безопасности как в международных, так и в национальных нормативно-правовых актах.
- 2. Развитие сотрудничества в этой сфере требует учет мнений всех заинтересованных сторон (правительств, бизнеса, технических и академических сообществ, структур гражданского общества).
- 3. Стоит задача обеспечения соответствия национальной практики международным нормам и стандартам в сфере кибербезопасности, формирование у населения культуры кибербезопасности.
- 4. Международно-правовые документы отстают от реального развития технологий и событий в сфере обеспечения кибербезопасности.
- 5. Необходимость усиления межгосударственного сотрудничества.
- 6. Актуализировался вопрос разработки всеобъемлющей международной конвенции о противодействии киберпреступности и обеспечении информационной безопасности.

БИБЛИОГРАФИЧЕСКИЕ ССЫЛКИ:

1. Резолюция ГА ООН 68/198 от 20 декабря 2013 года об использовании информационно-коммуникационных технологий (ИКТ) в целях развития // https://undocs.org/ru/A/RES/68/198.

2. Резолюция 71/199 ГА ООН от 19 декабря 2016 года о праве на неприкосновенность личной жизни в цифровой век // https://undocs.org/ru/A/RES/71/199.

3. Резолюция 68/243 ГА ООН от 27 декабря 2013 года о достижениях в сфере информатизации и телекоммуникаций в контексте международной безопасности // https://undocs.org/ru/A/RES/68/243.

4. Резолюция ГА ООН 57/239 ГА ООН от 20 декабря 2002 года о создании глобальной культуры кибербезопасности // https://undocs.org/ ru/A/RES/57/239.

5. Резолюция 56/121 ГА ООН от 23 января 2002 года о борьбе с преступным использованием информационных технологий // https://undocs.org/ ru/A/RES/56/121.

6. Резолюция 55/63 ГА ОНН от 22 января 2001 года о борьбе с преступным использованием информационных технологий // https://undocs.org/ru/A/RES/55/63.

7. Резолюция 130 Полномочной конференции Международного союза электросвязи (Дубай, 2018) усиление роли МСЭ в укреплении доверия и безопасности при использовании информационно-коммуникационных технологий // Заключительные акты Полномочной конференции Дубай 2018. С. 215–234 // https://www.itu.int/dms_pub/itu-s/opb/conf/S-CONF-ACTF-2018-R1-PDF-R.pdf.

8. Global Cybersecurity Index 2020. C.25-26 // https://www.itu.int/ dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf.

9. Конвенция о защите частных лиц в отношении автоматизированной обработки данных личного характера от 28 января 1981 года // https://rm.coe.int/1680078c46.

10. Дополнительный протокол к Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных, касающийся наблюдательных органов и трансграничной передачи данных (СЕД № 181) от 8 ноября 2001 года // https://rm.coe.int/1680080642.

11. Конвенция Совета Европы о компьютерных преступлениях от 23 ноября 2001 года // https://rm.coe.int/1680081580

12. Дополнительный протокол к Конвенции о преступлениях в сфере компьютерной информации, об инкриминировании расистских актов и совершенного ксенофоба при помощи информационных систем от 28 января 2003 года // https://rm.coe.int/1680081611.

13. Соглашение о сотрудничестве государств – участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации от 28 сентября 2018 года (г. Душанбе) // https://lex.uz/docs/4748982.

14. Решение Совета глав правительств СНГ о Стратегии сотрудничества государств – участников СНГ в построении и развитии информационного общества на период до 2025 года и Плане действий по ее реализации от 28 октября 2016 года // http://cis.minsk.by/reestr/ru/ index.html#reestr/view/text?doc=5490.

15. Соглашение между правительствами государств – членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности от 16 июня 2009 года // https://lex.uz/ru/docs/2068478.

16. Постановление Президента Республики Узбекистан от 21 ноября 2018 года № ПП-4024 «О мерах по совершенствованию системы контроля за внедрением информационных технологий и коммуникаций, организации их защиты» // https://lex.uz/docs/4071399.

17. Турсунов Ахтам Соломович и Абдулазиз Каримович Расулев. «Уголовно-правовые и криминологические меры борьбы с преступлениями в сфере информационных технологий и безопасности». Вопросы криминологии, криминалистики и судебной экспертизы 2 (2019): 40–44.

18. Расулев А.К. «Компьютерные преступления: уголовно-правовые и криминологические аспекты». (2006).

19. Расулев Абдулазиз Каримович. «Криминологическая характеристика преступлений в сфере информационных (компьютерных) преступлений». Вопросы современной юриспруденции 2 (53) (2016).