УДК 341.24:004-049.5
DOI: 10.36979/1694-500X-2026-26-3-109-116

# МЕЖДУНАРОДНО-ПРАВОВЫЕ ОСНОВЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ГОСУДАРСТВА

***А.Н. Иманкулова***

*Аннотация.* Рассматриваются особенности международно-правового регулирования информационной безопасности и международного сотрудничества в сфере защиты критически важных объектов национальных информационных систем. Проанализированы ключевые положения универсальных и специальных международных актов, регулирующих вопрос обеспечения информационной безопасности, в том числе резолюции Генеральной Ассамблеи ООН и договоры и соглашения региональных организаций. По результату анализа основополагающих международных документов в сфере информационной безопасности установлено, что в условиях активного формирования киберпространства возрастает проблема использования информационных технологий в противоправных целях. В данном контексте отмечается исключительная важность гармонизации национальных законодательств с общепризнанными международными нормами в борьбе с транснациональными преступлениями в информационной среде. Международные акты создают прочную правовую основу для разработки унифицированной политики ответственного поведения государств в информационной среде и способствуют укреплению глобальной информационной инфраструктуры.

*Ключевые слова:* безопасность; информация; информационная безопасность; информационное общество; кибербезопасность; международные акты; цифровизации; информационные технологии; государственная политика; жизненно важные интересы.

# МАМЛЕКЕТТИН МААЛЫМАТТЫК КООПСУЗДУГУН КАМСЫЗ КЫЛУУНУН ЭЛ АРАЛЫК-УКУКТУК НЕГИЗДЕРИ

***А.Н. Иманкулова***

*Аннотация.* Макала маалыматтык коопсуздукту эл аралык-укуктук жөнгө салуунун жана Улуттук маалыматтык тутумдардын маанилүү объектилерин коргоо чөйрөсүндөгү эл аралык кызматташтыктын өзгөчөлүктөрүнө арналган. Макалада маалыматтык коопсуздукту жөнгө салуучу универсалдуу жана атайын эл аралык актылардын негизги жоболору, анын ичинде БУУнун Башкы Ассамблеясынын резолюциялары жана аймактык уюмдардын келишимдери жана макулдашуулары талданган. Маалыматтык коопсуздук чөйрөсүндөгү негизги эл аралык документтерди талдоонун жыйынтыгы боюнча кибермейкиндикти Активдүү калыптандыруу шарттарында маалыматтык технологияларды укукка каршы максаттарда пайдалануу проблемасы өсүп жаткандыгы аныкталды. Бул контекстте Маалымат чөйрөсүндө трансулуттук кылмыштарга каршы күрөшүүдө улуттук мыйзамдарды жалпы таанылган эл аралык ченемдер менен шайкеш келтирүүнүн өзгөчө мааниси белгиленет. Эл аралык актылар мамлекеттердин маалыматтык чөйрөдө жоопкерчиликтүү жүрүм-турумунун бирдиктүү саясатын иштеп чыгуу жана глобалдык маалыматтык инфраструктураны чыңдоо үчүн күчтүү укуктук негизди түзөт.

*Түйүндүү сөздөр:* коопсуздук; маалымат; маалыматтык коопсуздук; маалыматтык коом; киберкоопсуздук; эл аралык актылар; санариптештирүү; маалыматтык технологиялар; мамлекеттик саясат; турмуштук кызыкчылыктар.

# THE INTERNATIONAL LEGAL FRAMEWORK FOR ENSURING THE INFORMATION SECURITY OF THE STATE

***A.N. Imankulova***

*Abstract.* The article is devoted to the peculiarities of international legal regulation of information security and international cooperation in the field of protection of critically important objects of national information systems. The article analyzes the key provisions of universal and special international acts regulating the issue of information security, including resolutions of the UN General Assembly and treaties and agreements of regional organizations. Based on the analysis of the fundamental international documents in the field of information security, it has been established that in the context of the active formation of cyberspace, the problem of using information technologies for illegal purposes is increasing. In this context, it is noted that it is extremely important to harmonize national legislation with generally recognized international norms in combating transnational crimes in the information environment. International acts create a solid legal basis for the development of a unified policy of responsible state behavior in the information environment and contribute to strengthening the global information infrastructure.

*Keywords:* security; information; information security; information society; cybersecurity; international acts; digitalization; information technology; public policy; vital interests.

В условиях активного развития информационных технологий и динамичного формирования нового глобального информационного пространства особую актуальность приобретает вопрос правового обеспечения информационной безопасности. Повсеместная информатизация общественных отношений, несмотря на очевидные положительные результаты, сопряжена с рядом новых угроз и вызовов, требующих пристального внимания со стороны международного сообщества. Современное общество зачастую сталкивается с несанкционированным нарушением целостности цифрового пространства, значительным снижением уровня защищенности информационных систем, новыми, ранее незнакомыми формами преступности и т. д. Кроме того, трансграничный характер подобных процессов свидетельствует о недостаточности использования лишь национальных механизмов их противодействия, в связи с чем возникает объективная необходимость разработки единообразных международных подходов в решении данных проблем.

В традиционном понимании информационная безопасность является неотъемлемым компонентом национальной безопасности государства и имеет системообразующее значение для устойчивого его развития [1, с. 1180]. Новые риски и угрозы, исходящие от информационного общества, предполагают расширение национальных интересов государств в рассматриваемой сфере и выход на международный уровень. В частности, некоторые авторы отмечают, что «…национальная безопасность государства существенным образом зависит от обеспеченности его международной информационной безопасностью» [2, с. 10]. В данном контексте усиливается роль международных актов, которые обеспечивают успешное функционирование субъектов в глобальном информационном пространстве.

Одним из ключевых международных документов, затрагивающих вопрос правового регулирования безопасности в информационной сфере, является *Всеобщая декларация прав человека* [3]. Этот акт закрепляет ключевые конституционные права и свободы человека, в том числе «искать, получать и распространять информацию и идеи любыми средствами и независимо от государственных границ» (ст. 19) [3]. Кроме того, Декларация защищает частную жизнь человека от незаконного вмешательства как непосредственного элемента информационной безопасности личности.

Нормы, закрепленные во Всеобщей декларации прав человека, находят свое логическое продолжение в специализированных международных актах, в том числе в сфере информационной безопасности. В частности, первым документом, направленным на организацию противодействия преступлениям в киберпространстве, признается *Конвенция о компьютерных преступлениях*, принятая Советом Европы в 2001 г. (Будапештская конвенция) [4]. Этот документ преследовал стратегическую цель – разработать унифицированные подходы в вопросе борьбы

с киберпреступлениями и гармонизировать национальные законодательства заинтересованных стран в соответствии с международными реалиями. В структурном плане нормы Будапештской конвенции охватывают три блока вопросов:

1. Уголовно-правовая характеристика ключевых киберпреступлений.

2. Особенности уголовно-процессуальных мер, используемых в борьбе с киберпреступлениями.

3. Организация международного сотрудничества в области противодействия киберпреступлениям.

Так, в первом блоке Конвенции содержится описание противоправных деяний, совершаемых в информационном пространстве, которые, по замыслу законодателя, рекомендуется признавать на национальном уровне в качестве уголовных преступлений. Исходя из объективной стороны данных деяний, Конвенцией предлагается выделение четырех основных групп компьютерных преступлений:

1. Преступления, направленные на разрушение целостности, доступности и конфиденциальности компьютерных данных и систем (противозаконный доступ, противозаконный перехват данных, нарушение целостности данных, вмешательство в функционирование системы, противоправное использование устройств);

2. Преступления, связанные с использованием компьютеров (подлог с использованием компьютеров, мошенничество с использованием компьютеров);

3. Преступления, связанные с нарушением данных (детская порнография);

4. Преступления, связанные с нарушением авторского или смежных прав [4].

Вопросы, касающиеся уголовной ответственности юридических лиц за указанные преступления (ст. 12) и установления соразмерных и эффективных мер наказания (ст. 13), относятся Конвенцией к ведению государств, ратифицировавших данный документ.

Одной из важных особенностей Будапештской конвенции является то, что ее положения не ограничиваются лишь описанием преступлений, совершаемых в информационном пространстве. Речь идет об уголовно-процессуальных механизмах расследования данных преступлений, содержащихся во втором блоке Конвенции. К примеру, в ст. 16 Конвенции указано, что важной составляющей обеспечения целостности информационных систем на национальном уровне является принятие законодательных или иных мер, способствующих сохранности компьютерных данных. В практическом плане данная мера может быть осуществлена посредством издания компетентными национальными органами соответствующего распоряжения «…какому-либо лицу об обеспечении сохранности конкретных хранимых компьютерных данных, находящихся во владении или под контролем этого лица» [4]. При этом обязанность лица обеспечивать надлежащий контроль за целостностью и сохранностью компьютерных данных ограничивается определенным сроком – не более девяноста дней. Как утверждают некоторые исследователи, указанный срок необходим для организации и проведения соответствующих процессуальных действий, например, обыска или изъятия компьютеров и др. [5, с. 307].

Помимо распоряжения об осуществлении контроля за компьютерными данными Конвенцией также предусматривается отдача распоряжения о предъявлении (ст. 18), согласно которому компетентные органы имеют возможность требовать от поставщиков услуг и других лиц предоставлять компьютерные данные, находящиеся в их владении или под их контролем. В данном случае запрашиваемые сведения могут включать в себя информацию об абонентах, т. е. «любую имеющуюся у поставщика услуг информацию в форме компьютерных данных или любой другой форме» [4]. Исключением являются сведения, с помощью которых можно установить личность самого абонента (к примеру, его номер телефона или адрес), тип предоставляемой услуги, место установки коммуникационного оборудования. Важно отметить, что такое распоряжение должно осуществляться исключительно на индивидуальной основе и в целях разрешения уголовного дела.

Следующие процессуальные нормы касаются «перехвата» данных о потоках информации (ст. 20) и данных о содержании (ст. 21), осуществляемого уполномоченными органами

либо поставщиками услуг в режиме реального времени с применением специальных технических средств. При этом «перехват» компьютерных данных подразумевает несколько альтернативных действий – сбор либо запись получаемых сведений. Несмотря на то, что указанные субъекты обязуются соблюдать принцип конфиденциальности осуществления этих операций, по своему содержанию они в значительной степени нарушают конституционное право человека на неприкосновенность его частной жизни, тайны личной корреспонденции. Как справедливо отмечают некоторые авторы, в данном случае подобные процессуальные действия должны осуществляться исключительно в отношении тяжких уголовных преступлений [5, с. 308].

Отдельные нормы Будапештской конвенции посвящены международному сотрудничеству в области совместной борьбы с киберпреступностью. Так, в ст. 23 определено, что международное сотрудничество в рассматриваемой сфере должно быть «максимально широким» и основываться на соответствующих международных договорах и соглашениях, а также нормах внутригосударственного права. Такое сотрудничество может быть организовано в виде взаимной правовой помощи, оказываемой государствами в целях проведения эффективного расследования уголовных преступлений, совершаемых с использованием различных компьютерных систем. В рамках организации расследования компьютерных преступлений в большинстве случаев международные запросы об оказании взаимной помощи затрагивают конституционные права и свободы индивида, в связи с чем Конвенцией предлагается осуществлять такую помощь посредством специально назначенных компетентных органов с каждой стороны. Эти органы обязуются оказывать друг другу информационно-техническое содействие, а также берут на себя полную ответственность за направление соответствующих запросов о взаимной правовой помощи и получение ответов на них (ст. 27). При этом важно подчеркнуть, что все процессуальные действия, осуществляемые как Запрашивающей, так и Запрашиваемой сторонами, должны обеспечивать сохранность и конфиденциальность передаваемых данных (ст. ст. 28,29).

Достаточно спорными по своему содержанию являются положения ст. 32 Конвенции, затрагивающие вопрос трансграничной передачи компьютерных данных. Так, согласно данной статье, «одна Сторона без согласия другой Стороны может получать доступ к общедоступным (открытому источнику) компьютерным данным независимо от их географического местоположения, а также получать через компьютерную систему на своей территории доступ к хранящимся на территории другой Стороны компьютерным данным или получать их…» [4]. Эта норма, по справедливому замечанию некоторых российских экспертов, является противоречивой, поскольку существенным образом нарушает не только принцип государственного суверенитета в информационном пространстве, но и фундаментальные основы правового статуса личности, в том числе в сфере частной жизни [6, с. 265]. Фактическим образом Будапештская конвенция предоставляет возможность какому-либо государству и его уполномоченным органам иметь бесконтрольный доступ к информационным системам и компьютерным данным другого государства без необходимости получать соответствующее разрешение на эти действия. Несмотря на то, что подобная практика существенным образом может облегчить процесс расследования компьютерных преступлений, она содержит в себе значительные угрозы возможной потери массива информационных данных, в том числе содержащих государственную тайну или другие охраняемые законом сведения. В этой связи, опасаясь потери государственного информационного суверенитета, многие страны мира (в т. ч. Кыргызская Республика) отказались ратифицировать нормы Будапештской конвенции.

Учитывая, что Конвенция против киберпреступлений была принята более двадцати лет назад, ее положения в современных условиях бурного развития и совершенствования информационных технологий не в полном объеме отвечают требованиям правового обеспечения глобального информационного пространства. В этой связи целесообразно рассматривать данный документ в качестве рамочного акта, заложившего прочную основу для создания более универсальной нормативно-правовой базы.

Важная роль в обеспечении информационной безопасности на международном уровне принадлежит Организации Объединенных Наций (далее – ООН), которая приняла ряд стратегических документов для создания международно-правового режима информационного пространства. Так, 4 декабря 1998 года Генеральной Ассамблеей ООН был принят первый нормативно-правовой акт в сфере глобальной информационной безопасности – *Резолюция A/RES/53/70 «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности»* [7]. Инициатором данного документа выступила Российская Федерация (далее – РФ), которая призывала государства-члены ООН в многостороннем формате «рассмотреть существующие и потенциальные угрозы в сфере информационной безопасности» [8]. Резолюция содержит ряд ключевых положений, в том числе о значительной потенциальной угрозе использования информационно-коммуникационных технологий в военных целях, целесообразность разработки международных стандартов в области противодействия применения информационного оружия, а также координации усилий по созданию единой площадки для обмена национальным опытом развития информационного пространства. Кроме того, авторами Резолюции предложены определения новых понятий, таких как «информационная война» и «информационное оружие».

По своему характеру Резолюция носила рекомендательный характер и послужила отправной точкой для формирования международной практики в сфере кибербезопасности. Так, следующим шагом ООН в обеспечении информационной безопасности в международном пространстве стало создание Группы правительственных экспертов (далее – ГПЭ), первая рабочая встреча которой состоялась в 2004 г. В рамках своей деятельности ГПЭ придерживается ключевого принципа консенсуса, позволяющего укреплять доверительные отношения между ее участниками в вопросах ответственного поведения в информационном пространстве. Данный принцип в полном объеме находит свое отражение в принятом ГПЭ *Кодексе поведения* (2013 г.) [9, с. 227–231], содержащем базовые принципы и правила безопасности субъектов в киберпространстве, меры по предотвращению возникновения и распространения киберугроз. Важным достижением в деятельности ГПЭ является создание самостоятельного института по обеспечению международной информационной безопасности – Рабочей группы ООН открытого состава (далее – РГОС). В отличии от ГПЭ РГОС предоставляет возможность участия в ее открытых сессиях всем государствам-членам ООН. Для укрепления международного сотрудничества в области информационной безопасности также была создана Группа высокого уровня по цифровому сотрудничеству, которая объединяет усилия не только правительств государств-участниц ООН, но и представителей гражданского общества, частного сектора, научного сообщества и др. [10].

«Переломным» событием в развитии системы международного сотрудничества в области информационной безопасности стало распространение короновирусной инфекции COVID-19. Переход в «онлайн-режим» способствовал активизации преступного поведения и появлению новых, более усовершенствованных видов транснациональных преступлений, в том числе совершаемых в киберпространстве. В условиях действия таких новых угроз международным сообществом были разработаны очередные стратегически важные документы – *Резолюция ГА ООН «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности»* (2019 г.), *доклад РГОС ООН по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности* (2021 г.).

Немаловажное значение в обеспечении информационной безопасности на международном уровне имеют документы, принятые Советом Безопасности ООН (далее – СБ ООН). Так, в *Резолюции 2341 (2017) СБ ООН* [11] подчеркивается, что одной из главных угроз международной безопасности, в том числе в информационной сфере, является террористическая деятельность в любых формах ее проявления. В этой связи СБ ООН обращает свое внимание на объективную необходимость обеспечения эффективных систем защиты критически важных объектов

инфраструктуры от терроризма и кибератак, а также создания прочной основы для развития международного сотрудничества в области противодействия подобным транснациональным преступлениям. При этом совместные усилия стран должны носить комплексный характер и затрагивать различные сферы, в том числе разведывательную и контрразведывательную деятельность, обмен информационными данными, управление рисками, обеспечение целостности и конфиденциальности информационных систем, защиту персональных данных и др. Учитывая, что в современных условиях террористические объединения обладают значительным техническим потенциалом, Резолюция также призывает страны-участницы ООН усиливать партнерские отношения между правительствами, частным сектором и региональными организациями (к примеру, ШОС или ОДКБ), вкладывать инвестиции в развитие технологической составляющей информационных систем, разрабатывать современные образовательные программы для подготовки профессиональных кадров в области информационных технологий.

Несмотря на то, что принятие данного документа стало значительным шагом в организации единой политики по обеспечению защиты критически важных объектов инфраструктуры, в практическом плане реализация его норм сталкивается с рядом трудностей. Это обстоятельство обусловлено наличием «технологического неравенства» стран, а также асимметричностью киберугроз [12, с. 40]. В этой связи преодоление подобных препятствий требует от международного сообщества разработки четко согласованных действий и усиления сотрудничества между странами.

В условиях стремительного развития угроз киберпространства возрастает значимость региональных международных организаций, также активно участвующих в разработке стратегически важных документов в области обеспечения информационной безопасности. Так, одним из таких ключевых актов является *Соглашение о сотрудничестве государств-членов Шанхайской Организации Сотрудничества* (далее – ШОС) *в сфере международной информационной безопасности*, подписанного 16 июня 2009 года [13]. Данное Соглашение было принято для предотвращения использования информационно-коммуникационных технологий в противоправных целях, обеспечения единого подхода для борьбы с киберпреступлениями и укрепления международного сотрудничества в сфере информационной безопасности.

Подтверждая значимость разработки совместной политики в области обеспечения международной информационной безопасности, государства-члены ШОС обращают свое внимание на наличие реальных угроз в данной сфере, которые по своей природе могут «нанести серьезный ущерб безопасности человека, общества и государства в нарушение основополагающих принципов равноправия и взаимного уважения, невмешательства во внутренние дела суверенных государств, мирного урегулирования конфликтов, неприменения силы, соблюдения прав человека» [14]. Так, в ст. 2 Соглашения обозначены следующие виды угроз информационной безопасности: использование информационных технологий в военных целях; информационный терроризм; распространение вредоносной информации; угрозы техногенного характера и др. В данной статье также отмечается, что для успешного преодоления этих факторов государствам необходимо их признавать и понимать их природу.

По своему характеру положения Соглашения носят обязательный характер и требуют от государств-членов ШОС унификации правоприменительной практики в рассматриваемой области. Уникальность данного акта также заключается в открытости для присоединения к нему других государств, что, безусловно, свидетельствует о расширении проблемы международной информационной безопасности в глобальном аспекте.

Развивая идею о создании международной системы информационной безопасности, заложенной в рассматриваемом выше Соглашении, отдельные государства-члены ШОС разработали конкретные *Правила поведения в информационном пространстве* и представили их для обсуждения на очередном заседании ГПЭ ООН в 2011. В дальнейшем они были обновлены и приняты в качестве официального документа

на 69-й сессии ГА ООН 9 января 2015 года [15]. Основной целью данных Правил является закрепление ключевых прав и обязанностей государств в информационном пространстве, поощрение их ответственного поведения в рамках использования информационных технологий, а также укрепление сотрудничества в борьбе с реальными угрозами международной информационной безопасности.

Важной особенностью анализируемого документа является его «миротворческий характер». В частности, в разделе 2 Правил отмечается, что государства должны предотвращать использование информационных технологий в агрессивных целях, к примеру, для подрыва национального суверенитета и политико-экономической стабильности государств, разжигания ненависти на религиозной или национальной почве и др. Кроме того, Правила предполагают обязательство государств воздерживаться от применения силы в рамках разрешения международных споров, возникающих в информационной среде. Особое внимание уделяется соблюдению прав и свобод человека, признаваемых на международном уровне. В частности, в п. 7 Правил закрепляется, что права и свободы человека, которыми он обладает в оффлайн среде, в одинаковом объеме должны быть защищены и в информационном пространстве. В данном контексте упомянуто право человека свободно искать, получать, передавать и распространять информацию законным путем. При этом предоставление этого права сопряжено с высокой ответственностью и некоторыми ограничениями, в том числе связанными с обеспечением прав и свобод других людей, защитой национальной безопасности и общественного порядка. Правила также затрагивают вопросы наращивания технологического потенциала государств и преодоления «цифрового разрыва», организации культуры информационной безопасности, несения солидарной ответственности стран в международном управлении сетью Интернет, а также укрепления регионального и международного сотрудничества в указанной сфере.

Ключевая идея Правил в последующем была заложена в основу следующих стратегических документов ШОС – *Астанинской декларации глав государств – членов ШОС* (2017 г.) [16] и *Циндаоской декларации Совета глав государств – членов ШОС* (2018 г.) [17]. С принятием этих актов государства – члены ШОС подтвердили свою готовность к созданию открытой и безопасной информационной среды, организации коллективной борьбы с киберпреступлениями. Здесь также подчеркивается особая роль ООН в разработке унифицированных правил и принципов ответственного поведения государств в информационном пространстве.

Подводя итог изучению основополагающих международно-правовых актов в сфере обеспечения информационной безопасности, необходимо отметить следующее.

Во-первых, обеспечение информационной безопасности в современных реалиях не является вопросом исключительно одного государства. Учитывая стремительный рост информационных технологий и использование их в противоправных целях, достаточно актуальной признается проблема международно-правового регулирования информационной сферы. Эта область отличается высокой чувствительностью к различного рода угрозам и требует координации совместных усилий стран для создания безопасной информационной среды.

Во-вторых, международные акты в сфере информационной безопасности носят комплексный характер и содержат базисные принципы и механизмы организации международного информационного пространства. В большей степени эти положения были сформулированы под влиянием различных международных и региональных организаций, обращающих свое внимание на исключительную необходимость укрепления международного сотрудничества в данной сфере.

В-третьих, проблема обеспечения информационной безопасности международно-правовыми средствами тесно связана с вопросом транспарентности информационных национальных систем и «технологического разрыва» государств. В некоторых случаях транснациональная передача информационных данных и необходимость организации контроля со стороны других государств, как указано в ведущих международных актах, может расцениваться

как посягательство на цифровой суверенитет страны. В связи с этим возникает реальная объективная необходимость создания более унифицированных подходов, позволяющих укреплять доверительные отношения между государствами в данной сфере.

Поступила: 29.10.2025;
рецензирована: 12.11.2025; принята: 14.11.2025.

***Литература***

1. *Захаров С.В.* Информационная безопасность как составляющая национальной безопасности государства / С.В. Захаров // Экономика и социум. 2021. № 12 (91).
2. *Сагымбаев А.А.* Международная информационная безопасность: вызовы и проблемы / А.А. Сагымбаев, З.К. Кожомуратов, А.С. Курманкожоева, А.А. Сагымбаев // Известия НАН КР. 2024. № 2.
3. Всеобщая декларация прав человека. Принята резолюцией 217 А (III) Генеральной Ассамблеи ООН от 10 декабря 1948 года. URL: https://www.un.org/ru/documents/decl_conv/declarations/declhr.shtml (дата обращения: 02.08.2025).
4. Конвенция о компьютерных преступлениях. Принята Советом Европы 23 ноября 2001 года. URL: https://rm.coe.int/1680081580 (дата обращения: 02.08.2025).
5. *Шестак В.А.* Будапештская конвенция как основополагающий механизм противодействия киберпреступности: новации и перспективы международно-правового регулирования / В.А. Шестак // Образование и право. 2023. № 9.
6. *Данельян А.А.* Международно-правовое регулирование киберпространства / А.А. Данельян // Образование и право. 2020. № 1.
7. Резолюция A/RES/53/70 «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности». URL: https://docs.un.org/ru/A/RES/53/70 (дата обращения: 03.08.2025).
8. *Бойко С.* Международная информационная безопасность: Россия в ООН. Начало истории (1998–2009 гг.) / С. Бойко // Международная жизнь. 2023. URL: https://interaffairs.ru/news/show/43346 (дата обращения: 03.08.2025).
9. Международная информационная безопасность: Теория и практика: сборник документов (на русском языке): в 3 т. Т. 2. / под общ. ред. А.В. Крутских. 2-е изд., доп. М.: Аспект Пресс, 2021. 784 с.
10. Группа высокого уровня Генерального секретаря ООН по цифровому сотрудничеству. URL: https://www.un.org/ru/sg-digital-cooperation-panel (дата обращения: 04.08.2025).
11. Резолюции 2341 (2017), принята Советом Безопасности ООН на его 7882-м заседании 13 февраля 1987 года. URL: https://mumcfm.ru/d/Xm7o2bzjQRvDdkXXpVq1ASrDO3xOmdCHwbwMRMVl (дата обращения: 04.08.2025).
12. *Чернявская К.Ю.* Деятельность ООН в информационном пространстве: история и документальная база организации в сфере борьбы с киберпреступностью / К.Ю. Чернявская // Русская политология. 2022. № 4 (25).
13. Соглашение между правительствами государств-членов Шанхайской Организации Сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности от 16 июня 2009 года. URL: https://ccdcoe.org/uploads/2018/11/SCO-090616-IISAgreementRussian-1.pdf (дата обращения: 06.08.2025).
14. *Бойко С.* Проблематика международной информационной безопасности на площадке ШОС и БРИКС / С. Бойко // Международная жизнь. 2019. № 1. URL: https://interaffairs.ru/jauthor/material/2131 (дата обращения: 08.08.2025).
15. Правила поведения в области обеспечения международной информационной безопасности. URL: file:///C:/Users/user/Downloads/A%2069%20723%20Ru.pdf (дата обращения: 08.08.2025).
16. Астанинская декларация глав государств – членов Шанхайской организации сотрудничества. URL: http://www.kremlin.ru/supplement/5206 (дата обращения: 08.08.2025).
17. Циндаоская декларация Совета глав государств – членов Шанхайской организации сотрудничества. URL: http://www.kremlin.ru/supplement/5315 (дата обращения: 08.08.2025).