

DOI 10.35775/PSI.2025.117.5.033

УДК 32.327

Д.А. КАРЕТНИКОВА

стажер-исследователь

Национального института исследований

глобальной безопасности (НИИГлоБ),

Россия, г. Москва

E-mail: karetnickowa.darya@yandex.ru

МЕЖДУНАРОДНАЯ ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ КАК ФАКТОР РОССИЙСКО-ТУРЕЦКОГО ДИАЛОГА: ПРЕДЕЛЫ И ВОЗМОЖНОСТИ

Статья анализирует проблемы и перспективы российско-турецкого сотрудничества в сфере международной информационной безопасности (МИБ) в условиях сложной геополитической обстановки. Рассматриваются как факторы, способствующие сближению (экономические интересы, борьба с терроризмом и киберпреступностью), так и препятствия (исторические противоречия, членство Турции в НАТО, различные позиции по международным вопросам). Представлены возможные направления укрепления взаимоотношений, особенно в энергетической сфере. Автор отмечает, что перспективы российско-турецкого сотрудничества в сфере МИБ остаются неопределенными и зависят от множества факторов. С одной стороны, общие экономические интересы и необходимость противодействия общим угрозам сближает страны. С другой стороны, исторические противоречия, геополитическая ориентация Турции на Запад и ее амбиции в регионе создают серьезные препятствия этому сближению. Несмотря на существующие риски и вызовы, автор считает, что сотрудничество в сфере МИБ может стать важным фактором стабильности и безопасности в регионе, если обе страны проявят политическую волю и готовность к компромиссам.

Ключевые слова: ИКТ, МИБ, кибербезопасность, Россия, Турция, КИИ, киберугрозы, энергетическое сотрудничество.

Российская Федерация и Турецкая Республика имеют долгую историю взаимоотношений со своими взлетами и падениями. Однако в последние пятнадцать лет Россия и Турция, налаживая тесные политические и экономические связи, сотрудничают в различных сферах: оборона, энергетика, финансы. В связи с этим, вопрос обеспечения информационной безопасности для двух держав становится более актуальным, так как необходимость защищать совместные проекты, деятельность, общую «чувствительную» информацию от современных информационных угроз все больше и больше возрастает.

МИБ или кибербезопасность: дилемма терминологии. Если сравнивать подходы зарубежных и российских авторов [11. С. 6] к политике государств в сфере безопасности информации на международном уровне, то становится очевидным, что российское понимание этого данного вопроса шире и конкретнее. Именно Россия первая из государств обратила внимание на появление угрозы национальной и международной безопасности в связи со стремительным развитием информационных технологий. Термин «международная информационная безопасность» впервые был официально использован в 1998 году при подписании президентами Российской Федерации и США текста Совместного заявления о регулировании проблем международной информационной безопасности [15. С. 200].

Российская Федерация подходит к определению понятия «международная информационная безопасность», основываясь на глобальном характере данной проблемы, учитывая не только технические, но и политико-идеологические угрозы. Под техническими угрозами российская сторона понимает угрозу безопасности и защищенности информационных сетей и систем. Политико-идеологические и политико-психологические угрозы – это манипулирование информацией, пропаганда противоправных, экстремистских идей, информационное воздействие на общественное сознание и т.д. [16. С. 81].

США и западные страны, а также и Турция, являясь членом североатлантического альянса, придерживаются более узкого подхода, делая акцент именно на технологических угрозах в данной сфере, поэтому используют термин «кибербезопасность». Об этих различиях свидетельствует и информация, изложенная в стандартах Международной Организации по Стандартизации (ISO), а именно в Руководящих указаниях по кибербезопасности в контексте ISO 27032 [10. С. 29].

Следует отметить, что сторонников подхода к проблеме международной информационной безопасности, предложенной Россией, с каждым годом становится все больше. Но в официальных документах ООН используется обобщенный рамочный термин – «безопасность в сфере использования информационно-коммуникационных технологий (ИКТ) и самих ИКТ» [11. С. 6].

Различия в подходах России и Турции. У России и Турции имеются как сходства, так и различия в подходах к основам обеспечения информационной безопасности.

Основные отличия заключаются в следующем:

1. Использование различной терминологии: информационная безопасность в России и кибербезопасность в Турции.

«Турецкая модель обеспечения кибербезопасности» создавалась с учетом опыта и передовых технологий западных стран. Будучи членом блока НАТО, Турция использует его наработки в сфере информационной безопасности и участвует в совместных «киберучениях» [14. С. 23].

2. В России существует более комплексный взгляд на вопрос обеспечения информационной безопасности, и она выступает за создание единого подхода к проблеме в мировом масштабе.

Россия первой поняла, какая угроза может быть от всеобщей компьютеризации и то, что избежать ее можно только приложив совместные усилия, приняв общие и юридически обязывающие к исполнению правила по поддержанию стабильности и безопасности международной цифровой среды в рамках ООН [26. С. 57]. Именно в данном направлении в настоящее время идет инициированный Российской Федерацией процесс создания системы информационной безопасности в таких международных региональных организациях, как ОДКБ и ШОС.

В Турции же не сразу смогли оценить значимость совместной деятельности в сфере информационной безопасности, но ситуацию изменили неоднократные попытки разрушить дружеские отношения и деловые контакты между Россией и Турцией путем распространения дезинформации через социальные сети.

3. Структуры Министерства обороны Российской Федерации (РФ) в области информационной безопасности нацелены на защиту отечественного информационного пространства, тогда как в Турции провозглашена, кроме защиты, наступательная идея в определении задач киберкомандования, созданного в Турции в 2012 году.

Также отличительной чертой турецкого подхода является привлечение хакеров к обеспечению ИБ страны. В Турции действует киберармия, получившая название «киберянычары». Общая численность киберспециалистов превышает 13 тысяч человек, причем включая бывших хакеров, которых называют «белыми», так как они добровольно перешли в государственные структуры информационной безопасности [9. С. 7].

В России же в 2014 году были созданы войска информационных операций в соответствии с приказом Министра обороны РФ С.К. Шойгу. В составе Генерального Штаба Вооруженных Сил РФ также было создано кибернетическое командование, призванное защищать электронные системы управления России от несанкционированного вмешательства [7].

К сходству позиций двух стран по информационной защите следует отнести единое понимание актуальности обеспечения информационной безопасности, которую Россия и Турция рассматривают как защиту информационной инфраструктуры и противодействие враждебным киберугрозам. Турция также, как и Россия, признает необходимым международное сотрудничество в сфере информационной безопасности. Поэтому между странами не прекращаются взаимоотношения даже в период нестабильности международной обстановки.

Современное состояние сотрудничества. Двустороннее сотрудничество России и Турции не прекратилось даже в условиях жесткого противостояния между странами Европейского союза во главе с США и Москвой. Как известно, Турецкая Республика не подключилась к антироссийским санкциям и даже пытается выступать посредником в диалоге между Россией и Украиной. С одной

стороны, Россия и Турция осознают, что их сотрудничество является важным условием стабильности на Ближнем Востоке, в Центральной Азии, Причерноморье и Кавказе, где влияние двух стран сильно и позиции по ряду вопросов совпадают. С другой стороны, успешное противостояние России международным вызовам и угрозам, делает нашу страну привлекательным партнером для Турции. Так, в 2022 году Россия выстояла в развязанной против нее кибервойне и смогла отразить до миллиона кибератак в неделю, включая DDoS-атаки на ряд российских правительственных информационных ресурсов и критическую информационную инфраструктуру страны [27. С. 6].

Для Турции вопрос сотрудничества с Россией в области информационной безопасности является чрезвычайно важным, так как между двумя странами существует целый ряд соглашений в энергетическом, военно-промышленном и финансово-экономическом секторе, где без защиты объектов КИИ не может идти и речи о безопасности. Турция ежегодно наращивает поставки газа из России. В частности, по газопроводу «Турецкий поток» из России в Турцию поступает 31,5 млрд кубометров газа в год, а через «Голубой поток» – 16 млрд кубометров [27. С. 7]. После подрыва в 2022 году «Северных потоков» и попытки совершения диверсии на газопроводе системы «Южный коридор», по которой газ поступает в Турцию, сотрудничество между странами вышло на новый уровень, а укрепление безопасности таких объектов КИИ стало еще более актуальным. Как заявил пресс-секретарь Президента РФ Д. Пескова, В. Путин и Р. Эрдоган обсуждали «возможность повышения уровня защиты газопровода «Турецкий поток» [17]. На современном этапе идет процесс переговоров России и Турции о создании на территории последней газового хаба [13. С. 114].

Кроме того, примером успешного сотрудничества является русско-турецкое межправительственное соглашение по строительству и эксплуатации АЭС «Аккую», в рамках которого реализуется модель «build-own-operate» («строй-владей-эксплуатируй») [14. С. 23]. По условиям данной модели, Россия не только реализует строительство, но и является владельцем будущей АЭС, Турция же гарантирует, что будет закупать электроэнергию. Проект «Росатома», безусловно, выгоден России, но и турецкая сторона также в этом заинтересована – после «завершения строительства «Аккую» все ее четыре реактора будут полностью обеспечивать энергией Стамбул и на 10% всю Турцию» [18]. Примечательным является и тот факт, что в 2022 году «Росатом» уже провел обучение российско-турецкого персонала по линии обеспечения информационной безопасности на данной АЭС. Сотрудники успешно изучили вопросы защиты компьютерных систем ядерных объектов по требованиям МАГАТЭ, а также на конкретных примерах разобрали ситуации по оценке угроз в компьютерных системах на основе общемировой практики противодействия таким угрозам [19].

Важным направлением российско-турецких взаимоотношений в настоящее время является военно-политическое сотрудничество. Особенно тесным оно стало после попытки военного переворота в Турции летом 2016 года. Турция приняла решение о закупке российских зенитно-ракетных комплексов (ЗРК)

С-400 «Триумф», в системе управления которого заложены современные российские программные комплексы, информационные системы и алгоритмы [3. С. 28].

Как известно, соглашение о поставке ЗРК С-400 «Триумф» было принято в 2017 году, и это был самый крупный контракт России со страной-членом НАТО о поставке вооружения. Всего Россией было поставлено в Турцию четыре дивизиона ЗРК на сумму 2,5 млрд долларов. Данное решение показало намерение Р. Эрдогана проводить самостоятельную политику без оглядки на Вашингтон и блок НАТО.

Еще одним важным аспектом взаимоотношений Турции и России является проблема борьбы с угрозой терроризма и экстремизма, включая информационное пространство. В 2021 году был заключен договор между Турцией и Россией по совместной работе в сфере противодействия террористическим действиям и киберпреступлениям. Началом взаимодействия двух стран в этом направлении стала программа на 2021-2022 гг. по сотрудничеству в борьбе с терроризмом и киберпреступностью. Программа затрагивала юридические аспекты, поэтому ее подписали Генеральный прокурор России Игорь Краснов и Заместитель Министра юстиции Турции Якуп Могул. Были намечены совместные действия по борьбе с киберпреступлениями, особое внимание предполагалось уделять «технологиям искусственного интеллекта и расчетам в криптовалюте, которые уже давно используют в качестве средства совершения киберпреступлений в разных странах мира» [14. С. 23].

В 2022 году состоялся первый визит генерального прокурора РФ в Турцию в рамках данного сотрудничества. И. Краснов отметил, что позиции Анкары и Москвы в вопросе борьбы с терроризмом, незаконным оборотом наркотиков, нелегальной миграцией и киберпреступностью достаточно схожи. Был подписан новый план по сотрудничеству в сфере противодействия преступлениям, совершаемым с использованием информационно-коммуникационных технологий, в том числе связанных с цифровыми финансовыми активами, а также вопросы, связанные с экстрадициями и с оказанием взаимной правовой помощи по уголовным делам на 2023-2024 гг. [22].

Кроме того, 21 июля 2021 года в России был принят Федеральный закон «О деятельности иностранных лиц в информационно-телекоммуникационной сети «Интернет» на территории Российской Федерации» [23], обязывающий иностранные интернет-компании оформлять юридическое лицо на территории РФ, а также размещать на своем ресурсе электронную форму для обратной связи с российскими гражданами или организациями. Сделано это было для того, чтобы уравнивать российские и иностранные IT-компании в их деятельности, распространить юрисдикцию РФ на иностранные компании для соблюдения ими всех требований, запретов и ограничений, предусмотренных законодательством РФ, и контролировать на этих платформах поток информации, которая порой носит экстремистский характер. В список таких организаций, обязанных оформить юридическое лицо в России, попали 20 иностранных компаний,

включая Facebook (2), Instagram (2), X (Twitter), TikTok, Google, YouTube, WhatsApp, Viber, Telegram, World of Tanks [17]. Интересен тот факт, что данный закон был разработан, опираясь на опыт Турецкой Республики, на основе аналогичного закона, согласно которому до 95% трафика компаний, не исполняющих местное законодательство, может быть заблокировано на территории Турции. Был проведен ряд консультаций с турецкими специалистами и профильными юристами [6].

Центробежные факторы взаимоотношениях России и Турции. Наличие многовекторных отношений между Россией и Турцией не означает, что между странами отсутствуют центробежные силы. Исторически сложилась ситуация соперничества между странами в Причерноморском регионе, на Ближнем Востоке и Кавказе. В Турции всегда будут помнить, что «история подъема Российской империи – это история упадка Османской империи» [24. С. 88], до сегодняшнего дня в Турции сохранились и популярны идеи возвращения утраченных земель. Обе страны предпочитают не затрагивать тему исторического прошлого, хотя итоги русско-турецких войн известны всем.

Не обозначая проблему исторического прошлого на межправительственных встречах двух стран, в самой Турции на самом высоком уровне вспоминают былое величие Порты. Например, в 2016 году на заседании Совета Безопасности страны Р. Эрдоган указал на то, что из 20 млн квадратных километров территории Османской империи осталось всего 720 тысяч, принадлежащих современной Турции, заверив: «Мы выйдем за границы нынешней территории, кто бы что ни говорил» [1. С. 27]. Данное заявление Россия вполне может воспринимать как угрозу своей территориальной целостности и как подрыв российского влияния на постсоветском пространстве.

Для этого есть все основания, так как Р. Эрдоган является активным сторонником идеи пантюркизма, возникшей еще в дореволюционный период в Османской Империи и ставящей задачу создания тюркского квази-государства под названием Великий Туран, которое должно объединить все тюркские народы, включая и проживающих на территории современной России (башкир, татар, чувашей) [12. С. 116]. Подтверждением этого является тот факт, что в ноябре 2021 года на саммите в Стамбуле была создана Организация Тюркских Государств (ОТГ) и принят официальный программный документ «Видение тюркского мира – 2040».

Проблема сотрудничества в области международной информационной безопасности заключается также в том, что Россия и Турция состоят в разнополярных блоках. Являясь членом блока НАТО, Турция должна противостоять Российской Федерации, против которой вся деятельность НАТО и направлена. Однако в действительности этого не происходит. Более того, Турция стремится проводить самостоятельную политику без оглядки на НАТО и США, сделав акцент на проблемы региональной безопасности, поэтому начиная с 2015 года выстраивает новую модель взаимоотношений с Россией [24. С. 89].

Разворот Турции в сторону России является непростым решением, так как ставит под вопрос информационную безопасность Турецкого государства, использующего программное обеспечение, полностью соответствующее стандартам НАТО. Это может привести к такой технической проблеме во взаимоотношениях двух стран, как обеспечение интероперабельности данных.

Центробежным фактором во взаимоотношениях двух стран является также то, что Россия и Турция занимают совершенно разные позиции по ряду международных проблем на Кавказе, Ближнем Востоке, Украине. Несмотря на все дружеские заверения в адрес России и российского президента, Турция не признает присоединение Крыма к Российской Федерации, периодически призывая «страны Запада не забывать о российской «аннексии»» [4]. Противоречивой является и позиция Турции по оценке СВО, с одной стороны Анкара призывает к миру и пытается выступать посредником по мирным переговорам, обмену пленными, а с другой стороны поставляет вооружение Украине [20], способствуя дальнейшей эскалации конфликта.

Кроме того, амбициозная внешнеполитическая деятельность Турции в соответствии с «Доктриной Эрдогана» (1) является проблемой сближения двух стран в сфере информационной безопасности. Россия постоянно испытывает угрозу со стороны НАТО, и Турция, как член этого блока и как самостоятельная сила, воспринимается Россией в качестве ситуационного союзника. Поэтому Российская Федерация создала зону эшелонированной обороны, развернув сети А2/AD (3) на Кавказе, в Сирии и в Крыму, находящуюся в непосредственной близости к границам Турции, что последнюю очень беспокоит [24. С. 91].

Перспективы сотрудничества и пределы невозможного. В настоящее время вопрос о возможности сотрудничества по вопросам международной информационной безопасности между Россией и Турцией экспертами оценивается по-разному, но в целом невысоко. Например, С.А. Шерстюков и Н.В. Бодиштану убеждены, что «у сближения России и Турции есть определенные пределы и, вероятно, эти пределы уже достигнуты» [24. С. 93]. Однако необходимость сотрудничества двух стран в сфере безопасности признается как фактор «устойчивости системы международной безопасности», а имеющийся опыт успешного сотрудничества может быть фактором сохранения его и в дальнейшем [2. С. 25].

Перспективы дальнейшего сотрудничества будут зависеть от общей международной ситуации и положения в регионах, представляющих взаимный интерес для Турции и России – Причерноморье, Кавказе, Ближнем Востоке. К укреплению сотрудничества Турцию могут подтолкнуть разумные и привлекательные предложения России по безопасности глобального информационного пространства.

Россия считает, что возможности для доступа в Интернет-пространство для всех стран должны быть равны, но каждое государство должно иметь суверенное право «управлять Интернетом в своем национальном сегменте»

[21]. Противоположной позиции придерживается США, выступая против национального регулирования информационного пространства, что дает стране-гегемону Интернета очевидные преимущества и ставит под угрозу информационную безопасность других стран. Турцию не может устраивать подобная ситуация, здесь ей ближе российские предложения, поэтому можно выйти на заключение двухсторонних соглашений между странами. Также Турция может подключиться к любой региональной организации, работающей на предложенных РФ принципах по обеспечению международной информационной безопасности, например ШОС.

Продолжение развития сотрудничества России и Турции по информационной безопасности может идти в энергетической сфере, так как после начала Специальной военной операции на Украине, Турция превратилась в важнейшего стратегического партнера России в области энергетики. На сегодняшний день «Турция является одновременно страной-потребителем энергоресурсов и страной-транзитером» [5. С. 472]. Разумеется, требования России по запрету совершения кибератак на критическую информационную инфраструктуру государства близки Турции [21]. Данная перспектива сотрудничества становится еще более очевидной после предложения, сделанного В.В. Путиным еще в 2022 году и подтвержденного в октябре 2023 года о создании в Турции газового хаба. Для Анкары предложение настолько выгодное, что Турция может забыть о некоторых идеях расширения своего влияния в регионе (но, к сожалению, не отказаться совсем).

Характер взаимоотношений России и Турции, напоминающий взлеты и падения, может быть сглажен расширением экономических связей [25. С. 333], выгодных обеим сторонам и имеющим множество сопутствующих факторов. Так, интенсификация связей в энергетике неизбежно приводит к установлению связей в других областях, в частности в вопросах обеспечения информационной безопасности и защиты КИИ. Например, «Росатом» уже провел обучение российско-турецкого персонала по линии обеспечения информационной безопасности на АЭС «Аккую» в 2022 году [19].

В настоящее время Россия может поставить Турции разработанные и проверенные средства защиты ИБ. Также в российских продуктах ИБ может быть заинтересован коммерческий сектор Турции, объем которого к 2026 году предположительно достигнет 598,4 млн долларов [11. С. 26].

Одной из перспективных областей сотрудничества Турции и России также становится военно-стратегический сегмент. Опыт сотрудничества уже есть и может быть продолжен, тем более что в противостоянии вооружениям стран блока НАТО российское выигрывает.

Кроме того, уже реализуемая и приносящая свои положительные результаты деятельность двух стран в сфере информационной безопасности по преодолению угроз терроризма и киберпреступности также может стать перспективным направлением развития дальнейшего сотрудничества.

Таким образом, перспективы взаимоотношений между Россией и Турцией в области МИБ зависят не только от самих стран, но и от международной обстановки, которая может как подтолкнуть страны друг к другу, так и отдалить, что уже было в истории российско-турецких отношений. Во избежание повторения ситуации охлаждения двухстороннего сотрудничества, могут помочь современные информационные технологии. По нашему представлению, это понимают и в Турции, и в России, поэтому перспективы сотрудничества в сфере МИБ очевидны. Такого же мнения придерживается политолог Р.И. Гайфутдинов, отмечая, что Турция умеет «преодолевать препятствия для сотрудничества в тех сферах, в которых потенциальные выгоды и общие интересы превалируют над разногласиями» [2. С. 26].

ПРИМЕЧАНИЯ:

- (1) Доктрина Эрдогана – ряд документов, обозначающих векторы внешне-политических действий страны, и заявлений Президента Турции на официальных мероприятиях, а именно: Документ о политике национальной безопасности, «Красная книга» Турции, Речь Р.Т. Эрдогана на заседании Генеральной Ассамблеи ООН в Нью-Йорке в 2021 году.
- (2) Признаны экстремистскими организациями и запрещены на территории РФ.
- (3) Сети A2/AD – анти-интервенционные зоны, создаваемые с помощью комплекса вооружений, которые при вторжении в данную зону нанесут неприемлемый ущерб противнику.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК:

1. Бдоян Д.Г. Проблемы российско-турецких отношений на современном этапе // Власть. 2017. Том 25. № 8.
2. Гайфутдинов Р.И. Внешняя политика Турецкой Республики в отношении Российской Федерации на современном этапе: специальность 5.5.4. «Международные отношения, глобальные и региональные исследования»: автореферат диссер. канд-та политических наук / Гайфутдинов Риналь Ильфатович. Москва, 2022.
3. Гасанов Р.Н. Российско-турецкое военно-политическое сотрудничество в современную эпоху // Азимут научных исследований: экономика и управление. 2021. Т. 10. № 1.
4. Глава МИД Турции призвал Европу не забывать об «аннексии Крыма» // РИА Новости // <https://ria.ru/20180608/1522319746.html>.
5. Гумбатов К.А. Особенности сотрудничества России и Турции в сфере энергетики // Московский экономический журнал. 2021. № 4.
6. Законопроект о приземлении зарубежных IT-гигантов – часть международной тенденции, считают российские эксперты // Интерфакс // <https://www.interfax.ru/presscenter/769158>.

7. Источник в Минобороны: в Вооруженных силах РФ созданы войска информационных операций // ТАСС // <https://tass.ru/politika/1179830>.
8. Как будет работать закон о «приземлении» IT-гигантов // Государственная Дума Федерального Собрания Российской Федерации // <http://duma.gov.ru/news/53199/>.
9. Ковалев О.Г., Скипидаров А.А. Организационно-правовые особенности построения системы кибербезопасности в зарубежных государствах (на примере модели Турецкой Республики) // Столыпинский вестник. 2021. Т. 3. № 2.
10. Марков А.С., Цирлов В.Л. Руководящее указание по кибербезопасности в контексте ISO 27032 // Вопросы кибербезопасности. 2014. № 1 (2).
11. Международная информационная безопасность: подходы России. М.: МГИМО Университет, 2021.
12. Новые вызовы и угрозы безопасности РФ в условиях глобальных и локальных трансформаций: монография / кол. авторов; под общ. ред. С.В. Устинкина, А.В. Никитина. М.: РУСАЙНС, 2023.
13. Нуриев Б.Д., Поспелов С.В. Энергетическая политика Турецкой Республики: экспансия в Восточном Средиземноморье // Вестник университета. 2023. № 3.
14. Оценка потенциала российских решений в области кибербезопасности на международном рынке. М.: Фонд «Центр стратегических разработок», 2022.
15. Пелевина Е.С. Особенности системы информационной безопасности как элемента международной безопасности в современном мире // Теории и проблемы политических исследований. 2017. Том 6. № 1А.
16. Прохорова Д.А. Международная информационная безопасность как современная проблема // Информационное общество. 2022. № 5.
17. Россия и Турция усилят защиту «Турецкого потока» // Вестник Кавказа // <https://vestikavkaza.ru/news/rossia-i-turcia-usilat-zasitu-tureckogo-potoka.html>.
18. Сотрудничество России с Турцией в сфере энергетики // ТЕК-ALL.ru // <https://www.tek-all.ru/news/id9611-sotrudnichestvo-rossii-s-turtsiey-v-sfere-energetiki/>.
19. Специалисты АО «Аккую Нуклеар» прошли подготовку по основам физической ядерной и информационной безопасности АЭС // Техническая Академия Росатом // <https://www.rosatomtech.ru/media/news-article/specialisti-ao-akkuyu-nuklear-proshli-podgotovku-po-osnovam-fizicheskoy-yadernoy-i-informacionnoy-bezopasnosti-aes/>.
20. Стало известно о поставке Украине кассетных боеприпасов турецкого производства // Газета.ru // <https://www.gazeta.ru/army/news/2023/10/27/21589069.shtml>.
21. Толстухина А. Российские инициативы в сфере международной информационной безопасности. // РСМД // <https://russiancouncil.ru/analytics-and-comments/analytics/rossiyskie-initsiativy-v-sfere-mezhdunarodnoy-informatsionnoy-bezopasnosti/>.

22. У России с Турцией общий киберфронт // Коммерсантъ // <https://www.kommersant.ru/doc/5653446>.
23. Федеральный закон № 236-ФЗ «О деятельности иностранных лиц в информационно-телекоммуникационной сети «Интернет» на территории Российской Федерации» от 1 июля 2021 года // <http://publication.pravo.gov.ru/Document/View/0001202107010014?index=2>.
24. **Шерстюков С.А., Бодиштану Н.В.** Российско-турецкие отношения после 2015 г.: новые тренды, старые дилеммы // Мировая экономика и международные отношения. 2021. Т. 65. № 11.
25. **Эргашев А.С., Чертилин О.В.** Внешнеполитические отношения России и Турции: ретроспективный анализ и современные реалии // Вестник Российского университета дружбы народов. 2021. Т. 8. № 3.
26. **Ющенко В.А.** Международная информационная безопасность: общая характеристика и российский подход к изучению // Русская политология. 2018. № 4 (19).
27. **Яникеева И.О.** Российско-американские отношения в сфере обеспечения международной информационной безопасности // Мировая политика. 2022. № 4.

D.A. KARETNIKOVA

Intern-Researcher of the National Institute for Global Security Studies (NIGSS),
Moscow, Russia

INTERNATIONAL INFORMATION SECURITY AS A FACTOR IN RUSSIAN-TURKISH DIALOGUE: LIMITS AND OPPORTUNITIES

The article analyzes the problems and prospects of Russian-Turkish cooperation in the field of international information security (IIS) in a complex geopolitical situation. It considers the factors contributing to the rapprochement (economic interests, the fight against terrorism and cybercrime), as well as obstacles (historical contradictions, Turkey's membership in NATO, different positions on international issues). Possible directions for strengthening mutual relations, especially in the energy sector, are presented. The author notes that the prospects for Russian-Turkish cooperation in the field of IIS remain uncertain and depend on many factors. On the one hand, common economic interests and the need to counter common threats bring countries closer together. On the other hand, Turkey's historical contradictions, geopolitical orientation towards the West and its ambitions in the region create serious obstacles to this rapprochement. Despite the existing risks and challenges, the author believes that cooperation in the field of IIS can become an important factor for stability and security in the region if both countries show political will and readiness to compromise.

Key words: ICT, IIS, cybersecurity, Russia, Turkey, CII, cyberthreats, energy cooperation.