ОРИГИНАЛЬНАЯ СТАТЬЯ

DOI: 10.26794/2226-7867-2024-14-3-20-27
УДК 327(045)

Информационная безопасность Исламской Республики Иран

М.А. Майорова[a], А.Р. Ерманалиева[b]
[a]Российский университет транспорта (МИИТ), Москва, Россия;
[b]Российская академия наук (РАН), Москва, Россия

АННОТАЦИЯ

В данной статье рассматривается сущность информационной безопасности, а также ее место в системе национальной безопасности Исламской Республики Иран. Оцениваются основные вызовы и угрозы, с которыми сталкивается страна в этой сфере. В работе подробно анализируются меры, которые Иран принимает для защиты своего информационного пространства: разработка систем противодействия киберугрозам, создание инструментов для кибершпионажа и атак на критическую инфраструктуру потенциального противника, а также фильтрация контента, противоречащего исламским ценностям. Кроме того, изучаются механизмы и формы его сотрудничества с Россией и Китаем. Авторы рассматривают текущую ситуацию в области информационной безопасности в Иране, используя качественный и количественный методы источникового анализа. Исследование показывает, что страна вынуждена активно защищать информационное пространство, учитывая постоянные угрозы со стороны внешних акторов, включая спецслужбы США и их союзников.

Ключевые слова: Исламская Республика Иран; национальная безопасность; национальные интересы; информационная безопасность; кибербезопасность; информационное общество; угрозы; защита информации; КСИР

Для цитирования: **Майорова М.А., Ерманалиева А.Р. Информационная безопасность Исламской Республики Иран**. ***Гуманитарные науки. Вестник Финансового университета.*** **2024;14(3):20-27. DOI: 10.26794/2226-7867-2024-14-3-20-27**

ORIGINAL PAPER

Information Security of the Islamic Republic of Iran

M.A. Mayorova[a], A.R. Ermanalieva[b]
[a]Russian University of Transport (MIIT), Moscow, Russia;
[b]Russian Academy of Sciences (RAS), Moscow, Russia

ABSTRACT

This article examines the significance of information security and its place within the national security framework of the Islamic Republic of Iran. It assesses the main challenges and risks that the country faces in this area. The paper provides a detailed analysis of measures taken by Iran to protect its information environment, including the development of systems to combat cyber threats, creation of tools for cyber-espionage and attacks against critical infrastructure of potential adversaries, as well as content filtering that contradicts Islamic values. Additionally, mechanisms and forms of cooperation with Russia and China are examined. The authors utilize qualitative and quantitative analysis of sources to assess the current state of information security in Iran. The study reveals that the country must actively protect its information sphere given the continuous threats posed by external actors, such as US intelligence agencies and their allies.

Keywords: Islamic Republic of Iran; national security; national interests; information security; cybersecurity; information society; threats; information protection; IRGC

For citation: **Mayorova M.A., Ermanalieva A.R. Information security of the Islamic Republic of Iran.** ***Gumanitarnye Nauki. Vestnik Finansovogo Universiteta = Humanities and Social Sciences. Bulletin of the Financial University.*** **2024;14(3):20-27. DOI: 10.26794/2226-7867-2024-14-3-20-27**

Национальная безопасность — способность нации удовлетворять потребности, необходимые для ее самосохранения, самовоспроизведения и самосовершенствования с минимальным риском ущерба для базовых ценностей ее нынешнего состояния. Она подразумевает состояние государства, при котором сохраняется его целостность и возможность быть самостоятельным субъектом системы международных отношений [1].

Иранский эксперт Насри Кадри, доцент кафедры политологии Университета имени Хорезми, отмечал, что сохранение национальной безопасности — это защита интересов государства и нации как в мирное, так и военное время [2]. Аятолла Хаменеи указывал, что культурная, экономическая, политическая, социальная, оборонная и экологическая сферы глубоко взаимосвязаны друг с другом и формируют национальную безопасность [3].

В настоящее время темы национальной и информационной безопасности тесно переплетаются из-за изменений, происходящих в современном обществе. Неоспоримо, что умение обрабатывать, анализировать и использовать информацию становится ключевым навыком. Современный человек, обладая доступом к многочисленным информационным ресурсам, выступает неотъемлемой частью глобальной системы, где данные взаимодействуют на различных уровнях.

В наши дни, когда СМИ играют значительную роль в определении границ и характера коммуникаций и взаимодействий в мировом сообществе, организации и международные юридические институты стремятся поддерживать и в некоторой степени управлять этой областью в соответствии с принципами защиты прав человека и свободы доступа к информации. Однако суверенитет и национальная безопасность имеют для государств такое же важное значение, и их нарушение недопустимо. Доцент кафедры права Университета Имама Хусейна Сохраб Салехи обращал внимание на то, что реализация принципа свободы информации может приводить к нарушению суверенитета и национальной безопасности, и при разработке стратегий это необходимо учитывать [4].

В политической сфере все большее значение приобретают не силовые, а информационные факторы [5]. В эпоху развития интернета и социальных сетей информация стала основным ресурсом — распространение фейковых новостей способно вызвать панику, нарушить стабильность общества и создать условия для возникновения национальных конфликтов.

Для борьбы с подобными угрозами важно формирование эффективной системы, включающей в себя разработку и реализацию мер по обнаружению, предотвращению и пресечению информационных атак, создание защищенной инфраструктуры для обмена информацией, обучение населения основам информационной безопасности, а также сотрудничество с другими странами в этой сфере [4].

ОПРЕДЕЛЕНИЕ И СУЩНОСТЬ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Сущность информационной безопасности (ИБ) заключается в обеспечении конфиденциальности, целостности и доступности информации, а также в защите от несанкционированного доступа, злоупотребления и повреждения данных [6].

Обеспечение ИБ основывается на следующих принципах [7]:

1. Принцип системности. Согласно ему, защитные меры должны быть нацелены на предотвращение информационных атак со стороны внешних и внутренних источников, а также учитывать каналы закрытого доступа и средства защиты. Последние надо использовать адекватно вероятным видам угроз, в комплексе, где они будут технически дополнять друг друга.

2. Принцип прочности. Устанавливает, что правила обеспечения ИБ должны охватывать все зоны безопасности, иметь равную надежность защиты и позволять определять вероятные угрозы.

3. Принцип многоуровневой защиты. Ориентирован на создание рубежей защиты информационной системы, состоящих из последовательно расположенных зон безопасности, ключевая из которых находится внутри всей системы.

4. Принцип бесперебойности. В соответствии с ним функционирование системы ИБ должно быть непрерывным и бесперебойным.

5. Принцип благоразумности. Выражается в разумности применения защитных мер с требуемой степенью безопасности. В его основе лежит целесообразность высоких материальных затрат и рациональность их дальнейшего

использования. Так, себестоимость защитных мер не должна превышать размер вероятного ущерба, расходы на обслуживание и работоспособность защитной системы [8].

В качестве основной меры защиты информации используется контроль доступа, призванный исключить возможность несанкционированного получения информации [9].

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В ИРАНЕ

Информационная безопасность в Иране представляет собой важную и сложную область, однако исследования научного характера по данной теме практически отсутствуют, поскольку это направление является относительно новым и пока неизученным.

Исламская Республика Иран уже 45 лет существует в условиях западных санкций, мирового давления и информационных войн, и, чтобы оказать достойное сопротивление, руководящей элите страны приходится концентрироваться на вооружении, разработке ядерного оружия, развитии киберпространства и науки. Исламский режим возник и заявил о себе как альтернатива «односторонней» глобализации (в ее вестернизованном варианте) в наиболее экстремальных формах [10].

Государство, находящееся с начала 1980-х гг. в сложной ситуации конфронтации с США, Израилем и арабскими странами Персидского залива, считает обеспечение безопасности в сфере информации одним из факторов геополитической устойчивости. Иран, официально причисленный США к «оси зла», стал одним из приоритетных объектов в информационной сфере для американских спецслужб и их союзников. Это стимулировало его развивать собственные возможности в области информационной безопасности, включая противодействие киберугрозам и информационным войнам, а также разработку систем для кибершпионажа и атак на объекты критической инфраструктуры потенциальных противников [11][1]. Для Ирана, как и для всех современных государств, возрастает зависимость функционирования системы государственного управления, социальной, экономической, транспортной и военной инфраструктуры от устойчивости и дееспособности обеспечивающей их инфраструктуры информационной.

Правительство ориентируется на приоритетное развитие эффективных механизмов по обеспечению контроля за интернет-пространством, мониторинга размещаемого контента и активности пользователей, чтобы предотвратить информационное воздействие на внутриполитическую ситуацию в стране.

Информационная безопасность регулируется рядом нормативно-правовых актов, которые направлены на обеспечение безопасности данных и информации в цифровой среде. Конституция Ирана устанавливает основы гарантий прав граждан на свободу слова и доступ к информации[2]. Закон «О компьютерных преступлениях», принятый в 2009 г., определяет их понятия и виды, а также предусматривает меры по их предотвращению и пресечению[3]. Кроме того, он устанавливает ответственность за нарушения в сфере компьютерной безопасности. В пунктах 7 и 8 Хартии прав граждан (2017 г.) содержатся положения, касающиеся обеспечения безопасности информации[4], а в Национальном законе об управлении данными и информацией — нормы по ее регулированию (2022 г.)[5].

Стратегия Исламской Республики Иран по информационной безопасности, в соответствии с решениями Высшего совета киберпространства, основывается на создании национальной интернет-сети с переключателями, маршрутизаторами и центрами обработки данных для того, чтобы запросы, поступающие из внутренних источников информации, обрабатывались внутри страны, обеспечивая полную автономию. Архитектура такой сети соответствует стандарту ISO/OSI. Для ее нормального функционирования необходим учет всех элементов инфраструктуры и пользовательского оборудования, а также гарантии безопасности на всех уровнях активности [12].

В Иране существует ряд ведомств, которые занимаются вопросами информационной без-

[1] URL: https://russiancouncil.ru/activity/digest/longreads/kibermoshch-irana/

[2] URL: https://worldconstitutions.ru/?p=83

[3] URL: https://spaceiran.com/computer-crime-laws

[4] URL: https://media.president.ir/uploads/ads/148214204462093500.pdf

[5] URL: https://www.shenasname.ir/laws/39164-%D 9%82%D 8%A7%D 9%86%D 9%88%D 9%86-%D 9%85%D 8%AF%D B%8C%D8%B 1%DB%8C%D 8%AA-%D 8%AF%D 8%A7%D 8%AF%D 9%87-%D 9%87%D 8%A7

опасности. В первую очередь, стоит отметить Министерство информации, которое координирует политику в области информационных технологий, разрабатывает специальные меры и отвечает за защиту от кибератак [13]. Национальный центр киберпространства также несет ответственность за координацию мер по обеспечению информационной безопасности. Узкую область — кибербезопасность регулирует Верховный совет по киберпространству (ВСК), основные задачи которого — блокировка нежелательных интернет-ресурсов и регулирование вопросов развития кибертехнологий. Данное ведомство функционирует под руководством аятоллы Али Хаменеи и состоит из глав служб разведки и безопасности, Корпуса стражей исламской революции (КСИР), судебной власти, Меджлиса (парламента), государственного радио и телевидения и т.д.

В настоящее время главным инструментом политики сопротивления является Корпус стражей исламской революции (КСИР) [14] –корпоративное объединение военных, разведывательных, полицейско-репрессивных, политико-идеологических, а также финансово-экономических структур. По сути, это многопрофильный мегахолдинг, руководимый непосредственно верховным лидером и его окружением. Сегодня КСИР — это становой хребет государственности Исламской Республики Иран, а также — государство в государстве [15].

Участие КСИР в обеспечении безопасности в сфере информационно-коммуникативных технологий (ИКТ) обосновывается необходимостью защиты страны от воздействия западных идей через интернет-ресурсы. США определила КСИР как движущую силу кибератак. По данным Управления национальной разведки США за 2021 г., «опыт и готовность Ирана проводить агрессивные кибероперации делают его серьезной угрозой для безопасности сетей и данных США и союзников»[6].

Одна из частей, подконтрольных КСИР в сфере безопасности,— киберармия Ирана (Ir.CA)[7] — группа нелегальных программистов и технических специалистов (Black hat[8]), которые действуют в интересах государства. Они проводят мониторинг Интернета, организуют кибератаки на оппозиционные сайты и каналы. Организация также известна под другими названиями: APT33[9], Charming Kitten[10], Cobalt Dickens[11] и пр. Однако на официальном уровне Иран отрицает свою причастность к ней. Одной из причин является желание сохранить планирование и проведение кибератак в тайне, чтобы не привлекать внимание международного сообщества и не подвергать себя риску международных санкций[12].

В 2011–2013 гг. наблюдалось увеличение частоты и интенсивности сетевых атак со стороны Ирана[13], в частности — на финансовую систему США. В рамках данной кампании иранские хакеры успешно выводили из строя веб-платформы финансовых институтов, создавая значительные проблемы для экономической стабильности США.

Иранские службы безопасности неоднократно демонстрировали серьезные навыки в проведении подобных атак. В 2018 г. Министерство юстиции США обвинило Иран в краже данных из сотен университетов, компаний и государственных учреждений[14]. В 2019 г. хакеры из вышеупомянутой иранской группы Cobalt Dickens атаковали более 60 университетов в США[15].

На фоне усиления санкций США и роста напряженности в Персидском заливе, летом 2019 г. Иран предпринял попытку кибератаки на Бахрейн, где базируется пятый флот ВМС США и Центральное командование ВМС. Другой целью иранских хакеров стало Управление электроэнергетики и водоснабжения Бахрейна,

[6] URL: https://www.dni.gov/index.php/newsroom/reports-publications/reports-publications-2023/3676–2023-annual-threat-assessment-of-the-u-s-intelligence-community

[7] URL: https://ebrary.net/173527/political_science/islamic_republic_iran_s_cyber_security_strategy_challenges_cyber_uncertainty

[8] Black hat — термин, который обычно используется для обозначения хакеров, занимающихся киберпреступлениями.

[9] URL: https://ib-bank.ru/bisjournal/news/19523

[10] URL: https://russiancouncil.ru/analytics-and-comments/columns/cybercolumn/nikto-ne-znaet-o-persidskikh-kotakh-gruppirovka-charming-kitten-i-strategiya-bezopasnosti-tegerana/?sphrase_id=131615498

[11] URL: https://xakep.ru/2019/09/12/cobalt-dickens/

[12] URL: https://blog.sekoia.io/iran-cyber-threat-overview/

[13] URL: https://www.justice.gov/opa/pr/seven-iranians-working-islamic-revolutionary-guard-corps-affiliated-entities-charged

[14] URL: https://www.justice.gov/opa/pr/nine-iranians-charged-conducting-massive-cyber-theft-campaign-behalf-islamic-revolutionary

[15] URL: https://cyberscoop.com/cobalt-dickens-iran-universities-hacking-secureworks/)

алюминиевый завод (Aluminium Bahrain) и национальная нефтяная компания Bapco. Атаки нарушили работу этих объектов, уничтожив или удалив важные для их функционирования данные[16].

В конце 2020 г. на израильскую компанию Clear Sky, специализирующуюся на кибербезопасности, было совершено несколько серий атак с распространением сообщений-угроз. Данные действия были произведены Ираном с целью внушить страх и оказать психологическое давление на врага[17].

В 2024 г. новостной сайт The Hacker News выпустил пост о серии кибератак на Албанию, осуществленных Ираном, обвинив его в использовании вредоносных программ (No-Justice Wiper (NACL.exe) и PowerShell) для удаления данных с компьютеров и распространения через сеть. Целями атак были телекомпания One Albania, телекоммуникационная компания Eagle Mobile Albania, флагманский авиаперевозчик Air Albania и парламент страны[18].

В Иране используется несколько подходов для обеспечения информационной безопасности. Один из них — ограничение доступа к определенным сайтам и социальным сетям, например, к таким популярным платформам, как Facebook, X (Twitter) и YouTube[19]. Другой — фильтрация интернет-трафика, когда с помощью программного обеспечения блокируются сайты, которые не соответствуют правительственной политике[20]. В стране на основе технологий Deep packet inspection[21] проводится серьезная работа по очищению интернет-пространства и политика цензурирования. Третий подход подразумевает создание отдельной национальной сети, предназначенной для обмена информацией между государственными организациями и предоставления гражданам доступа к государственным ресурсам. Иранское правительство активно занимается созданием «халяльного Интернета», который будет обеспечивать безопасность и защиту интересов государства[22]. В рамках этой инициативы также реализуется проект «чистого интернета», который позволит более эффективно бороться с преступностью и выявлять нарушителей закона. Так, была разработана система идентификации «Шахкар» (Shakhkar), которая следит за отправителями и получателями данных по IP-адресам[23].

В 2009 г. в Иране был принят закон «О компьютерных преступлениях[24]» для обеспечения правового регулирования в вопросах безопасности в сфере ИКТ. Данные меры связаны с «зеленым движением», участники которого выступали против подтасовок результатов президентских выборов в 2009 г. В ходе протестов активно использовались социальные сети (в том числе Facebook и Twitter), чтобы поддерживать связь с внешним миром. В результате в начале 2011 г. руководство страны объявило о начале функционирования нового подразделения киберполиции для проведения контрразведки и пресечения любых видов кибершпионажа[25].

В рамках борьбы с протестами и бунтами производится отключение Интернета в активных зонах. В ноябре 2019 г. Тегеран приказал интернет-провайдерам заблокировать доступ в сеть по всей стране, поскольку демонстрации из-за скачков цен на топливо переросли в политические протесты[26]. В иранской провинции Хузестан в июле 2021 г. во время выступлений, вызванных нехваткой воды[27], также случались перебои в работе Интернета. В обоих случаях действия властей были направлены на то, чтобы не допустить мятеж и предотвратить гражданскую войну.

В марте 2021 г. КСИР, в соответствии с заявлениями Али Хаменеи о том, что интернет «не

[16] URL: https://www.zdnet.com/article/new-iranian-data-wiper-malware-hits-bapco-bahrains-national-oil-company/
[17] URL: https://therecord.media/israel-shipping-logistics-watering-hole-cyberattacks
[18] URL: https://thehackernews.com/2024/01/pro-iranian-hacker-group-targeting.html
[19] URL: https://www.rbc.ru/spb_sz/24/09/2012/55929cea9a794719538c5114?from=copy
[20] URL: https://rsf.org/en/how-islamic-republic-has-enslaved-iran-s-internet
[21] URL: https://ooni.org/post/2018-iran-protests-pt2/
[22] URL: https://rsf.org/en/iran-creates-halal-internet-control-online-information
[23] URL: https://russiancouncil.ru/analytics-and-comments/columns/sandbox/politika-iranskogo-pravitelstva-po-uregulirovaniyu-kiberprostranstva/
[24] URL: https://spaceiran.com/computer-crime-laws
[25] URL: https://phys.org/news/2011–01-iran-cyber-crime-police.html
[26] URL: https://netblocks.org/reports/internet-disrupted-in-iran-amid-fuel-protests-in-multiple-cities-pA25L18b)
[27] URL: https://netblocks.org/reports/mobile-internet-disrupted-in-iran-amid-khuzestan-water-protests-1yPjK9AQ

должен отдаваться на усмотрение врага», объявил об очистке сети от «пошлостей»[28,29].

Таким образом, иранские специалисты в последние годы продемонстрировали значительные улучшения своих технических навыков. Это выражается в их способности проводить сложные и качественные кибероперации, опасные для противников. Также в стране разработана четкая стратегия по фильтрации Интернета, созданию национальной сети, а все ведомства полностью взяты под контроль центрального аппарата.

СОТРУДНИЧЕСТВО В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Иран сотрудничает с несколькими странами в сфере информационной безопасности с целью обмена опытом, знаниями и совместной борьбы с угрозами. Россия — ключевой партнер иранской стороны. Тегеран и Москва имеют тесные связи в различных областях, включая информационную безопасность, поддерживают обмен информацией о выявленных киберугрозах и совместно работают над созданием средств защиты от кибератак. В январе 2021 г. страны подписали договор о координации своей кибердеятельности[30].

Другим не менее значимым партнером Ирана является Китай. Государства обмениваются опытом и знаниями о современных технологических угрозах, а также сотрудничают в области разработки и внедрения мер по защите информации и сетевой безопасности. Будучи крупным покупателем иранской сырой нефти и важным торговым партнером, Китай предоставил Ирану телекоммуникационное оборудование, а телекоммуникационные гиганты Huawei и ZTE уже почти десять лет поставляют иранскому правительству оснащение для наблюдения за текстовыми сообщениями, звонками и электронной почтой[31].

Иран взаимодействует с другими странами в сфере информационной безопасности, обмениваясь опытом и проводя совместные тренинги и учения. Однако сведений об этом в интернете мало, что может быть связано с необходимостью сохранения конфиденциальности, поскольку подобное сотрудничество осуществляется в рамках секретных или полусекретных межправительственных соглашений.

Подводя итоги, стоит отметить, что Исламская Республика Иран с момента своего существования принимает стратегические меры по обеспечению собственной информационной безопасности. Для страны важна защита своего информационного пространства, в том числе путем фильтрации контента, противоречащего исламским ценностям. Все ведомства и организации, занимающиеся подобной деятельностью, подчинены верховному лидеру Али Хаменеи, что гарантирует единство и централизацию в этой области, а также позволяет развиваться в едином направлении для защиты своих интересов.

[28] URL:https://www.jahannews.com/news/758317/%d9%81%d8%b6%d8%a7%db%8c-%d9%85%d8%ac%d8%a7%d8%b2%db%8c-%d9%88%d9%84%d9%86%da%af%d8%a7%d8%b1%db%8c-%d8%b1%d9%87%d8%a7-%d8%ae%d9%88%d8-%a7%d9%87%db%8c%d9%85

[29] URL:https://www.mehrnews.com/news/5174427/%D8%AA%D8%A3%DA%A9%DB%8C%D8%AF%D8%A7%D8%AA-%D9%85%D9%87%D9%85-%D8%B1%D9%87%D8%A8%D8%B1%DB%8C-%D8%AF%D8%B1%D8%A8%D8%A7%D8%B1%D9%87-%D9%85%D8%AF%DB%8C%D8%B1%DB%8C%D8%AA-%D9%81%D8%B6%D8%A7%DB%8C-%D9%85%D8%AC%D8%A7%D8%B2%DB%8C-%DA%86%DB%8C%D8%B3%D8%AA

[30] URL: https://tass.ru/politika/10548911

[31] URL: https://www.mei.edu/publications/25-year-iran-china-agreement-endangering-2500-years-heritage

СПИСОК ИСТОЧНИКОВ

1. Балашова Т.Н. Национальный интерес и национальная безопасность в контексте миграции населения: взаимосвязь и взаимодействие. *Общество и право.* 2008;(1):23–31.
2. Nasri K. Oil and National Security of the Islamic Republic of Iran. URL: https://www.researchgate.net/publication/278727046_Oil_in_the_Islamic_Republic_of_Iran_Dependence_Distortions_and_Distribution
3. Habibzadeh G. Dimensions of security from the perspective of Imam Khamenei. *National Security*. 2019;9(31):7–32.
4. Salahi S., Mazaheri M., Moradi M. Sovereignty and national security in the light of freedom of information. *Defense Policy*. 2018;27(108):75–116.
5. Богачев В.Я., Редин В.В. Информационная безопасность как составная часть национальной безопасности Российской Федерации. URL: https://cyberleninka.ru/article/n/informatsionnaya-bezopasnost-kak-sostavnaya-chast-natsionalnoy-bezopasnosti-rossiyskoy-federatsii

6. Farid G., Warraich N.F., Iftikhar S. Digital information security management policy in academic libraries: A systematic review (2010–2022). URL: https://www.researchgate.net/publication/333632477_httpsjournalssagepubcomdoifull10117701925121198294 75, URL: https://doi.org/10.1177/01655515231160026
7. Буйневич М.В., Покусов В.В., Израилов К.Е. Модель угроз информационно-технического взаимодействия в интегрированной системе защиты информации. *Информатизация и связь.* 2021;(4):66–73.
8. Буйневич М.В., Покусов В.В., Израилов К.Е. Способ визуализации модулей системы обеспечения информационной безопасности. *Вестник Санкт-Петербургского университета Государственной противопожарной службы МЧС России*. 2018;(3):81–91.
9. Зарипова Г.К., Рамазонов Ж.Ж. Информационная безопасность. *Научные исследования*.2019;(1):51–54.
10. Мамедова Н.М. Ислам и развитие Ирана в начале XXI века. *Россия и мусульманский мир.* 2006;(4):115–125.
11. Ковалев О.Г, Скипидаров А.А. Кибербезопасность в условиях национального интернета (Иранский опыт противодействия киберугрозам). *Столыпинский вестник.* 2021;3(3):186–195.
12. Ghorbani V., Saghafi K. Desien of Security Information Architecture Strategic Model for the Islamic Republic of Iran Cyberspace. *National Security.* 2020;10(37):85–126.
13. Taghipour R., Lashkarian H., Naseri A., Yazdani Ch.R. Critical Information Infrastructure Cyber-Protection Strategic in Islamic Republic of Iran. *National Security.* 2020;9(34):7–48.
14. Дунаева Е.В., Мамедова Н.М., Сажин В.И. Год после выхода США из ядерной сделки (новые риски для Ирана). *Восточная аналитика.* 2019;(1):76–90.
15. Сажин В.И. Корпус стражей исламской революции Ирана — государство в государстве. *Контуры глобальных трансформаций: политика, экономика, право.* 2017;(3):83–109. DOI: 10.23932/2542–0240–2017–10–3–83–109

REFERENCES

1. Balashova T.N. National interest and national security in the context of population migration: interrelation and interaction. *Obshchestvo i parvo = Society and law.* 2008;(1):23–31. (In Russ.).
2. Nasri K. Oil and national security of the Islamic Republic of Iran. URL: https://www.researchgate.net/publication/278727046_Oil_in_the_Islamic_Republic_of_Iran_Dependence_Distortions_and_Distribution (In Farsi).
3. Habibzadeh G. Dimensions of security from the perspective of Imam Khamenei. *National Security*. 2019;9(31):7–32. (In Farsi).
4. Salahi S., Mazaheri M., Moradi M. Sovereignty and national security in the light of freedom of information. *Defense Policy*. 2018;27(108):75–116. (In Farsi).
5. Bogachev V. Ya., Redin V.V. Information security as an integral part of the national security of the Russian Federation. URL: https://cyberleninka.ru/article/n/informatsionnaya-bezopasnost-kak-sostavnaya-chast-natsionalnoy-bezopasnosti-rossiyskoy-federatsii (In Russ.).
6. Farid G., Warraich N.F., Iftikhar S. Digital information security management policy in academic libraries: A systematic review (2010–2022). URL: https://www.researchgate.net/publication/333632477_httpsjournalssagepubcomdoifull10117701925121198294 75, URL: https://doi.org/10.1177/01655515231160026
7. Buinevich M.V., Pokusov V.V., Izrailov K.E. Threat model of information technology interaction in an integrated information security system. *Informatizaciya i svyaz' = Informatization and Communication.* 2021;(4):66–73. (In Russ.).
8. Buinevich M.V., Pokusov V.V., Izrailov K.E. A method for visualizing modules of an information security system. *Vestnik Sankt-Peterburgskogo universiteta Gosudarstvennoj protivopozharnoj sluzhby MCHS Rossii = Bulletin of the St. Petersburg University of the State Fire Service of the Ministry of Emergency Situations of Russia.* 2018;(3):81–91. (In Russ.).
9. Zaripova G.K., Ramazanov J.J. Information security. *Nauchnye issledovaniya = Scientific research.* 2019;(1):51–54. (In Russ.).
10. Mamedova N.M. Islam and the development of Iran at the beginning of the XXI century. *Rossiya i musul'manskij mir = Russia and the Muslim World*. 2006;(4):115–125. (In Russ.).
11. Kovalev O.G., Skipidarov A.A. Cybersecurity in the context of the national Internet (The Iranian experience of countering cyber threats). *Stolypinskij vestnik = Stolypin Bulletin.* 2021;3(3):186–195. (In Russ.).
12. Ghorbani V., Saghafi K. Desien of Security Information Architecture Strategic Model for the Islamic Republic of Iran Cyberspace. *National Security.* 2020;10(37):85–126. (In Farsi).

13. Taghipour R., Lashkarian H., Naseri A., Yazdani Ch.R. Critical information infrastructure cyber-protection strategic in Islamic Republic of Iran. *National Security.* 2020;9(34):7–48. (In Farsi).
14. Dunaeva E.V., Mamedova N.M., Sazhin V.I. The year after the US withdrawal from the nuclear deal (new risks for Iran). *Vostochnaya analitika = Oriental analytics.* 2019;(1):76–90.
15. Sazhin V.I. Iran's Islamic Revolutionary Guard Corps is a state within a state. *Kontury global'nyh transformacij: politika, ekonomika, parvo = The contours of global transformations: politics, economics, law.* 2017;(3):83–109. DOI: 10.23932/2542–0240–2017–10–3–83–109

ИНФОРМАЦИЯ ОБ АВТОРАХ / ABOUT THE AUTHORS

Мария Алексеевна Майорова — преподаватель кафедры «Международные отношения и геополитика транспорта», Российский университет транспорта (МИИТ), Москва, Россия
Mariya A. Mayorova — Lecturer at the Department of International Relations and Geopolitics of Transport, Russian University of Transport (MIIT), Moscow, Russia
https://orcid.org/0000-0003-0751-5210
Автор для корреспонденции / Corresponding author:
alex1996m5@inbox.ru

Аида Рамильевна Ерманалиева — старший лаборант Отдела Ближнего и Постсоветского Востока Института научной информации по общественным наукам, Российская академия наук (РАН), Москва, Россия
Aida R. Ermanalieva — Senior Laboratory Assistant at the Department of the Near and Post-Soviet East of the Institute of Scientific Information on Social Sciences, Russian Academy of Sciences (RAS), Moscow, Russia
https://orcid.org/0009-0003-8524-0141
lonny.bin21@mail.ru

Конфликт интересов: авторы заявляют об отсутствии конфликта интересов.
Conflicts of Interest Statement: The authors have no conflicts of interest to declare.

Статья поступила 11.04.2024; принята к публикации 11.05.2024.
Авторы прочитали и одобрили окончательный вариант рукописи.
The article was received on 11.04.2024; accepted for publication on 11.05.2024.
The authors read and approved the final version of the manuscript.