DOI: 10.31249/j.2949-2408.2025.02.09
УДК 327+339

РОССИЙСКИЕ ТЕХНОЛОГИИ – ИНВЕСТИЦИИ В НАЦИОНАЛЬНУЮ БЕЗОПАСНОСТЬ ИРАНА

ОБУХОВА Анастасия Николаевна
младший научный сотрудник Центра изучения стран
Ближнего и Среднего Востока Института востоковедения РАН
E-mail: anastasia.n.obukhova@yandex.ru
SPIN-код: 2846-0853
ORCID: 0009-0008-6232-172X

Для цитирования: *Обухова А.Н.* Российские технологии – инвестиции в национальную безопасность Ирана // Ближний и Постсоветский Восток. – 2025. – № 2 (10). – С. 111–128. – DOI: 10.31249/j.2949-2408.2025.02.09.

Аннотация. Укрепление национального цифрового суверенитета Ирана реализуется в сложных геополитических условиях, где требующие отражения непрерывные угрозы информационной безопасности носят глобальный характер. Вследствие вынужденной международной изоляции страны на протяжении более сорока лет, уровень решений по защите инфраструктуры информационной безопасности в стране остается недостаточно проработанным. В связи с этим Ирану необходимо создавать собственные функциональные программно-аппаратные решения для развития устойчивости собственной инфраструктуры к кибератакам. На сегодняшний день Россия достигла полной самообеспеченности по ключевым показателям устойчивости, у российских технологических компаний есть опыт работы в странах Азии, поэтому Россия может предложить Ирану как отечественные решения по кибербезопасности, так и другие технологии, в частности по микроэлектронике. Для России сотрудничество с Ираном в сфере технологий имеет большое значение как с точки зрения выхода на рынки «дружественных» стран в условиях формирования нового миропорядка, так и с точки зрения потенциально быстрой монетизации российских разработок на быстрорастущем рынке, каким является Исламская Республика Иран.

Ключевые слова: информационная безопасность Ирана, российские решения по кибербезопасности, российско-иранское технологическое сотрудничество.

Russian Technologies – Investments in Iran's National Security

Anastasia N. OBUKHOVA
Junior Researcher, Center for Middle East Studies,
Institute for Oriental Studies, Russian Academy of Sciences
E-mail: anastasia.n.obukhova@yandex.ru
SPIN-code: 2846-0853
ORCID: 0009-0008-6232-172X

For citation: Obukhova A.N. (2025). Russian Technologies – Investments in Iran's National Security. *Middle & Post-Soviet East*, no. 2 (10), pp. 111–128. (In Russ.) DOI: 10.31249/j.2949-2408.2025.02.09.

Abstract. Strengthening the national digital sovereignty of Iran is being implemented in difficult geopolitical environment amid constant threats of global nature to information security that need to be addressed. Due to the forced international isolation of the country for over forty years, the domestic solutions for protecting the information security infrastructure tend to be outdated. Thus, Iran must develop its own functional software and hardware solutions to increase the resilience of its own infrastructure to cyberattacks. Nowadays, Russia has achieved complete self-sufficiency in key areas, while Russian technology companies have experience working in Asian countries. As a result, Russia can offer Iran both domestic cybersecurity solutions and other technologies, in microelectronics. Russian cooperation with Iran in the field of technology is of great importance in terms of entering the "friendly" market amid the new world order formation and considering a potentially quick monetization in the fast-growing market.

Keywords: Iran's information security, Russian cybersecurity solutions, Russian-Iranian technological cooperation.

Укрепление национального цифрового суверенитета в Исламской Республике Иран (ИРИ) реализуется в сложных геополитических условиях, требующих отражения непрерывных угроз информационной безопасности глобального характера, критической необходимости импортозамещения цифровых платформ и сервисов, создания функциональных программно-аппаратных решений и развития устойчивости собственной инфраструктуры к кибератакам. В 2024 г. среди 188 стран Иран занял 91-е место в мире в «Глобальном индексе готовности правительств к искусственному интеллекту», поднявшись с 94-го места годом ранее[1]. Однако вследствие нахождения под международными санкциями и рестрикциями на протяжении более сорока лет, уровень решений по защите инфраструктуры информационной безопасности в стране отстает от российских.

[1] Иран улучшил позиции в Глобальном индексе готовности правительств к искусственному интеллекту // Информационное агентство Исламской Республики (ИРНА). – 24.02.2025. – URL: https://ru.irna.ir/news/85761070/Иран-Улучшил-Позиции-в-Глобальном-Индексе-Готовности-Правительств (дата обращения: 20.05.2025).

Несмотря на вынужденную изоляцию, в 2023 г. Иран стал четвертым в мире по темпам роста экономики с реальным ростом ВВП в 4,7% г/г, уступив только Индии (рост на 7,3%), КНР (рост на 5,3%), Индонезии (рост на 5,1%) (график 1). В 2024 г. рост иранской экономики превысил 3%[2].

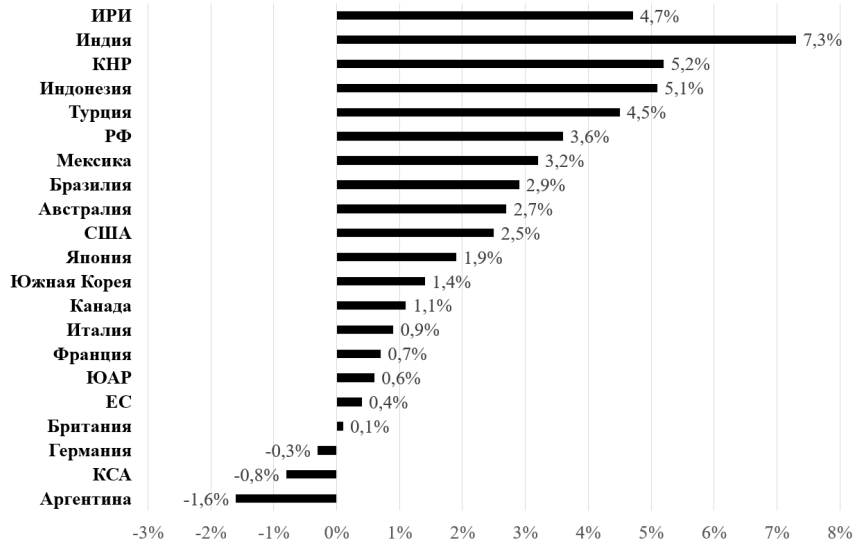

График 1. Реальный рост ВВП по странам, 2023 г.[3, 4]

Седьмой национальный план развития (2023–2027) Ирана прогнозирует рост иранской экономики на уровне 8% ежегодно, что непросто реализовать в условиях международных санкций и незаконных односторонних рестрикций со стороны стран Запада[5]. Пятилетний план предполагает увеличение объемов газодобычи до 1,34 млрд куб м / день, для достижения которых потребуются около 19 млрд долл. ежегодных инвестиций, а общие инвестиции необходимы в размере 75 млрд долл., включая 53 млрд долл. на разработку новых газовых месторождений и 22 млрд долл. – на

[2] Iran GDP Annual Growth Rate // Trading economics. – URL: https://tradingeconomics.com/iran/gdp-growth-annual (дата обращения: 10.03.2025).

[3] Западноевропейские страны в 2023 г. продолжили путь к деиндустриализации: ВВП Германии сократился на 0,3%, совокупный рост экономик ЕС – 0,4% => рынок сбыта для товаров из КНР, и потенциально для ресурсов ИРИ, сокращается.

В 2023 г. ВВП ИРИ вырос на 4,7% г/г, опередив рост экономики Турции (+4,5%), РФ (+3,6%), приблизившись к росту КНР (+5,2% г/г).

[4] World Economic Outlook Database: October 2024 Edition // IMF. – URL: https://www.imf.org/en/Publications/WEO/weo-database/2024/October (дата обращения: 14.03.2025).

[5] Economic Trends // Central Bank of the Islamic Republic of Iran. – URL: https://cbi.ir/category/EconomicTrends_en.aspx (дата обращения: 15.03.2025).

поддержание производственных мощностей, включая проект повышения давления на месторождении Южный Парс[6]. Кроме того, Ирану требуются около 4 млрд долл. инвестиций в течение 10 лет в судостроение и создание производства специализированной стали для судов, по оценкам главы Департамента морской промышленности Организации промышленного развития и реконструкции Мохаммада Эсмаили[7]. В целом для достижения своих экономических целей Ирану необходимо 200 млрд долл. инвестиций к 2031 г. (из которых 50% инвестиций может быть привлечено через фондовый рынок), по оценкам Ходжатолла Сейеди, главы Организации по ценным бумагам и биржам Ирана[8]. В этой связи инвестиции в информационную безопасность по защите существующей и вновь создаваемой критически важной инфраструктуры нефтяных и газовых трубопроводов, металлургических комбинатов, сайтов и серверов государственных и бюджетных организаций приобретают особую актуальность.

Для отражения киберугроз иранским государственным организациям, предприятиям, средним и малым предпринимателям (СМП) приходится действовать в трех направлениях. Это включает работу по противодействию атакам зарубежных преступных группировок, по нейтрализации действий киберпреступников, по борьбе с финансовым кибермошенничеством. Атаки на инфраструктуру национальной информационной безопасности приводят к утечке конфиденциальной информации, нарушению основной деятельности организаций, ущербу интересам государства (график 2).

Наибольше количество кибератак производят APT группировки (от англ. advanced persistent threat), т.е. группировки «постоянной серьезной угрозы», члены которых – высококвалифицированные хакеры, атакующие организации для получения конфиденциальной информации, имеющей существенное значение для реализации политических и экономических решений, работы ВПК. Основным инструментом нижеследующих APT-группировок является кибершпионаж. В Иране зафиксировано порядка 25 преступных групп, среди которых следует выделить следующие:

1. Группировка APT 15 имеет предположительно китайское происхождение, осуществляет кибершпионаж в отношении иранского правительства. Кибератиность APT 15 была отмечена во второй половине 2022 г., после чего в начале 2023 г. на иранскую инфраструктуру последовали кибератаки.

---

[6] Iran signs $17 b deal to boost gas pressure at South Pars field // Tehran Times – 08.03.2025. – URL: https://www.tehrantimes.com/news/510663/Iran-signs-17b-deal-to-boost-gas-pressure-at-South-Pars-field (дата обращения: 17.03.2025).

[7] Iran needs $4 b to expand maritime fleet: IDRO // Tehran Times. – 11.02.2025. – URL: https://www.tehrantimes.com/news/509633/Iran-needs-4b-to-expand-maritime-fleet-IDRO (дата обращения: 14.03.2025).

[8] Iran needs $200 b of investment by 2031 to achieve economic goals // Tehran Times. – 12.10.2024. – URL: https://tehrantimes.com/news/504858/Iran-needs-200b-of-investment-by-2031-to-achieve-economic-goals (дата обращения: 16.03.2025).

2. Группировка Bahamut действует в странах Ближнего Востока и Южной Азии и, в том числе осуществляя хакерские атаки на заказ.

3. Группировка Molerats атакует организации государственного сектора, предприятия ВПК и топливно-энергетического комплекса, заводы, средства массовой информации.

4. Группировка Desert Falcons осуществляет атаки на транспортную отрасль, школы, вузы, научные центры.

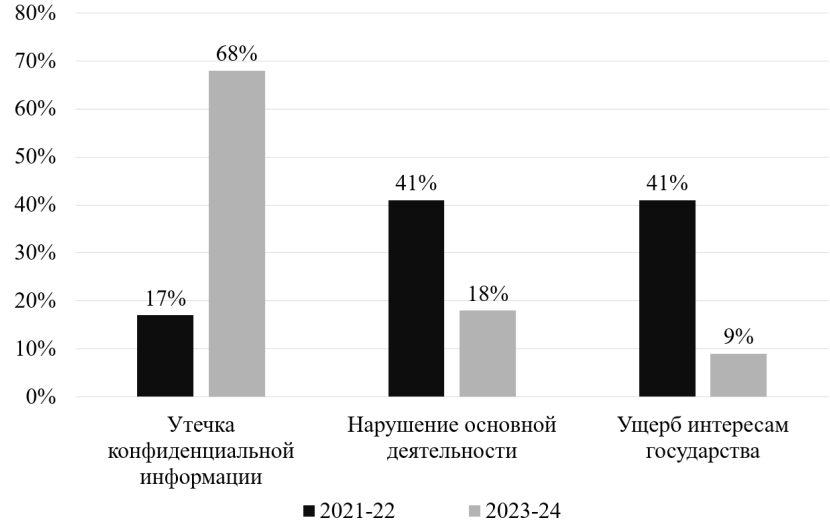

График 2. Последствия кибератак на организации ИРИ, 2021–2024 гг.[9]

Кроме того, в стране действуют так называемые хактивистские группировки, чья доля в общем количестве атак снизилась за 1,5 года (2023 – первую половину 2024 г.) на 15 п.п. Хактивисты отличаются от APT-группировок тем, что их действия мотивированы политически (а не финансово) и происходят из-за несогласия с геополитическими событиями в стране или регионе. За 2021–2022 гг. в Иране 42% кибератак хактивистов было направлено на госучреждения, и 40% – за 2023 год – первое полугодие 2024 г.[10] В Иране зафиксирована деятельность таких хактивистских группировок, как Black Reward, Tapandegan, Edalat-e Ali, GhostSec, Ghyamsarnegouni, Gonjeshke Darande (Predatory Sparrow) и WeRedEvils. Деятельность последней носит политический характер, а кибератаки осу-

[9] Ландшафт киберугроз в Иране: 2021 – H1 2024 // Позитивные Технологии. – 29.10.2024. – URL: https://www.ptsecurity.com/ru-ru/research/analytics/landshaft-kiberugroz-v-irane-2021-h1-2024/ (дата обращения: 02.03.2025).

[10] Там же.

ществляются на промышленную и телекоммуникационную инфраструктуры (взлом системы управления проектами нефтяной инфраструктуры Ирана). Кибератаки Predatory Sparrow (группировки предположительно израильского происхождения) направлены на иранские промышленные объекты (сталелитейные заводы и завод химической промышленности), железнодорожную инфраструктуру Ирана, АЗС и правительственную инфраструктуру (в 2022 г. в результате атаки группировки были нарушены технологические процессы трех иранских сталелитейных заводов, что вызвало пожар в одном из них). Группировка GhostSec атакует промышленные предприятия (в частности, в апреле 2024 г. путем атаки на иранского производителя электропанелей получила доступ к SCADA-системе).

На темпы роста кибератак влияет наличие геополитических конфликтов (график 3). В третьем квартале 2023 г. доля кибератак на Иран в ближневосточном регионе составляла 7%, на КСА – 8, на ОАЭ – 8, на Палестину – 5, на Израиль – 11%, а на все остальные страны приходилось около двух третей всех атак[11]. В результате событий 7 октября 2023 г., доля кибератак на Израиль (среди стран Ближнего востока) выросла до 49%, на Палестину – до 10 в четвертом квартале, и доля Ирана размылась до 5, КСА – до 5, ОАЭ – до 3, остальных стран – до 28%.

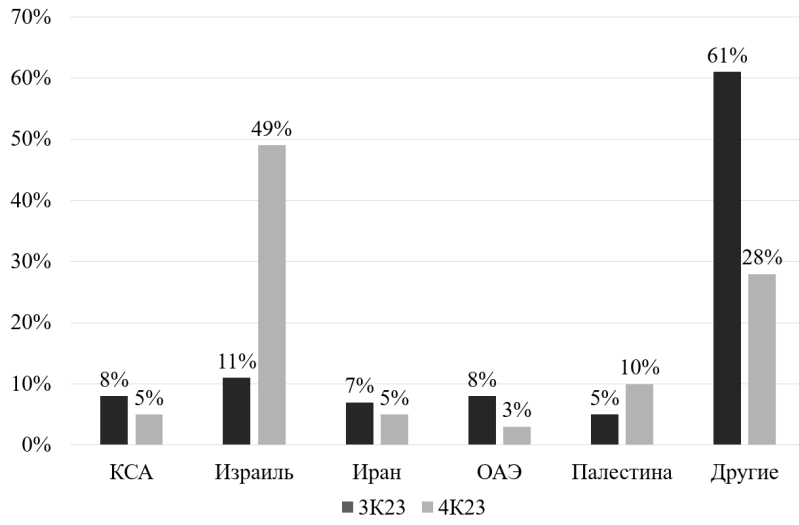

График 3. Доля кибератак по странам: ИРИ, ОАЭ, Палестина, КСА, Израиль в 3 и 4 кварталах 2023 г.[12]

[11] Актуальные киберугрозы на Ближнем Востоке: 2023–2024 // Позитивные Технологии. – 18.10.2024. – URL: https://www.ptsecurity.com/ru-ru/research/analytics/aktualnye-kiberugrozy-na-blizhnem-vostoke-2023-2024/ (дата обращения: 04.03.2025).
[12] Там же.

Среди методов воздействия хактивистских групп наиболее востребованы DDoS-атаки на веб-сайты организаций и их дефейс, а также использование дарквеба («теневого интернета») для объявлений, где преобладают доли объявлений таких хактивистов, как Arvin Club (21%), группировки YourAnonUKRIR (16%), финансово мотивированной группировки Ares и хактивистов GhostSec (по 8%)[13]. Последняя в феврале 2024 г. выложила в дарквебе объявление, демонстрирующее результат кибератаки на иранский сталелитейный завод с помощью вайпера (график 4).

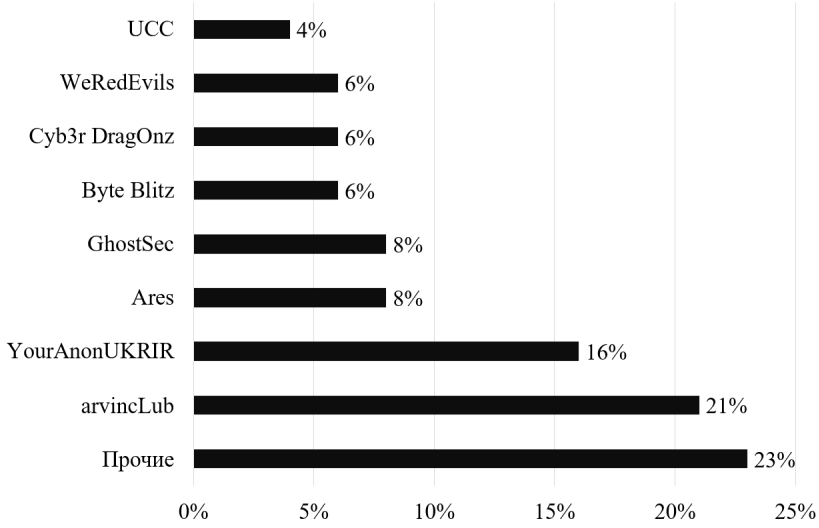

График 4. Объявления в иранском дарквебе, 2023–2024 гг.[14]

Почти в половине объявлений киберпреступники публиковали новости о взломе организации; 24% – по продаже украденных данных (БД и доступа к инфраструктуре организаций), 22% – объявления о бесплатной раздаче украденных данных. В частности, в результате атаки на страховые компании Ирана в декабре 2023 г. хакер опубликовал в дарквебе объявление о продаже свыше 160 млн записей с данными из 23 ведущих страховых иранских компаний[15].

[13] Чурсина А. Страны Персидского залива как товар на рынке преступных киберуслуг (анализ 2023–2024 годов) // Позитивные Технологии. – 18.09.2024. – URL: https://www.ptsecurity.com/ru-ru/research/analytics/gulf-countries-as-a-commodity-in-the-market-on-criminal-cyber-services-2023-2024/#id1 (дата обращения: 01.03.2025).
[14] Ландшафт киберугроз в Иране: 2021 – H1 2024 // Позитивные Технологии. – 29.10.2024. – URL: https://www.ptsecurity.com/ru-ru/research/analytics/landshaft-kiberugroz-v-irane-2021-h1-2024/ (дата обращения: 02.03.2025).
[15] Там же.

Наиболее часто применяющийся инструмент хактивистов в Иране – вредоносное программное обеспечение (ВПО), использующееся практически в двух кибератаках из трех (график 5). Для сравнения: доля использования ВПО в атаках на российские компании составила 62% в 2024 г.[16] Примечательна и другая тенденция в действиях хактивистов в Иране и на Ближнем Востоке – снижение доли DDoS-атак. Это происходит из-за роста числа финансово мотивированных киберпреступлений и хактивизма: кражу конфиденциальных данных или шифрование данных компании можно монетизировать (например, продать базу данных), в отличие от вывода из строя веб-ресурса или компонентов инфраструктуры (за что с жертвы невозможно получить вознаграждение).

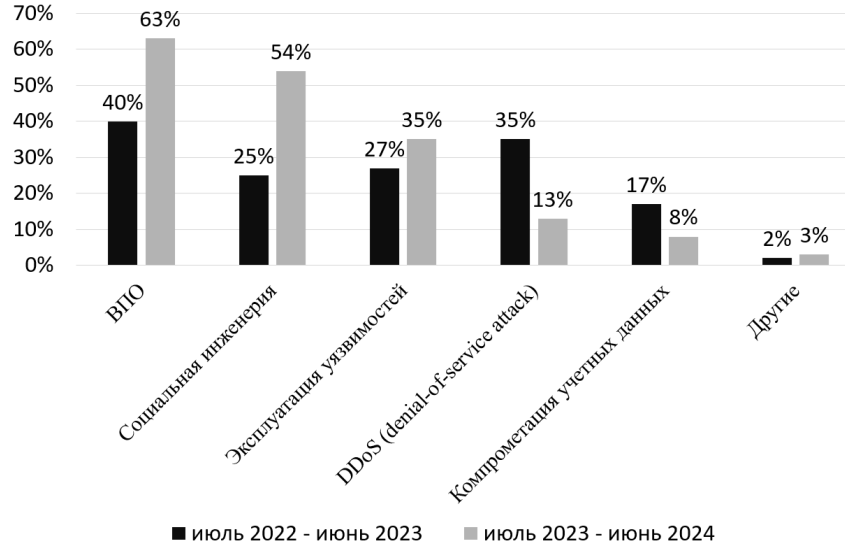

График 5. Инструменты кибератак в ближневосточном регионе, июль 2022 г. – июнь 2024 г.[17]

Также отмечается рост использования официально установленного программного обеспечения (приложения банков, мониторинговых организаций) при осуществлении атак преступниками за 1,5 года (с 2023 г. по

[16] Российский рынок ИБ и его роль в мировой индустрии: итоги 2024 года и прогнозы на 2025 // Позитивные Технологии. – 18.12.2024. – URL: https://www.ptsecurity.com/ru-ru/research/analytics/rossijskij-rynok-ib-i-ego-rol-v-mirovoj-industrii-itogi-2024-goda-i-prognozy-na-2025/#id2 (дата обращения: 05.03.2025).

[17] Актуальные киберугрозы на Ближнем Востоке: 2023–2024 // Позитивные Технологии. – 18.10.2024. – URL: https://www.ptsecurity.com/ru-ru/research/analytics/aktualnye-kiberugrozy-na-blizhnem-vostoke-2023-2024/ (дата обращения: 04.03.2025).

первое полугодие 2024 г.). При этом преступники осуществляют взлом этих приложений для распространения вирусов, антиправительственных призывов и т.п. Помимо этого, в стране растет доля банковских троянов, которые скрывают свое присутствие на зараженных ими устройствах, встраиваются в модульную бот-сеть, где вредоносные характеристики добавляются через модули или библиотеки.

Региональной особенностью хакеров, действующих на Ближнем Востоке, является активное использование так называемых вайперов (вредоносное программное обеспечение, удаляющее данные), доля которых выросла с 3% в 2021–2022 гг. до 8% в первом полугодии 2024 г.[18] Вайперы удаляют данные, пользовательские и системные файлы, что позволяет преступникам вывести из строя оборудование. Поэтому наибольшую опасность несет попадание вайпера на устройства автоматизированной системы управления технологическим процессом и в инфраструктуру промышленных систем, оснащенную устройствами IoT (internet of things – «интернет вещей»). На Ближнем Востоке наибольшее количество таких устройств в июне 2024 г. было зафиксировано в Иране (график 6).

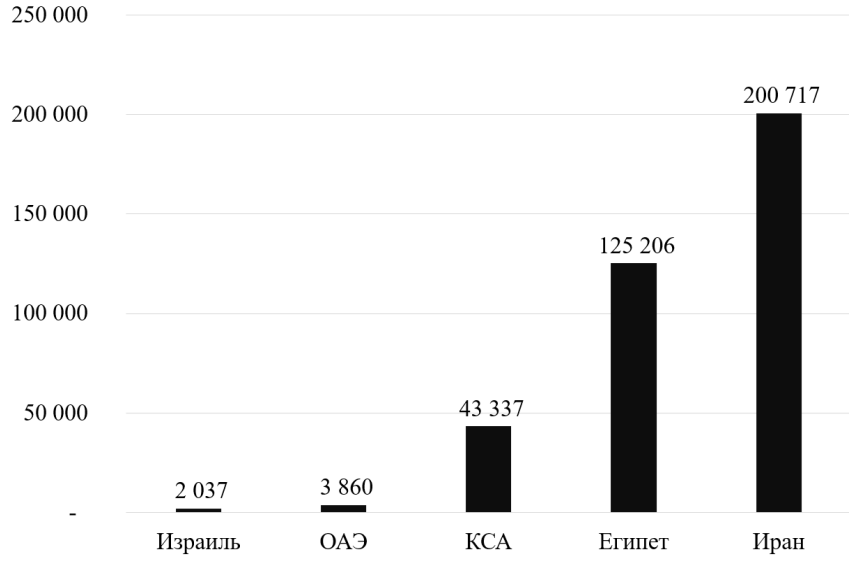

График 6. Число устройств «интернет вещей»
в странах Ближнего Востока в первом полугодии 2024 г.[19]

[18] Актуальные киберугрозы на Ближнем Востоке: 2023–2024 // Позитивные Технологии. – 18.10.2024. – URL: https://www.ptsecurity.com/ru-ru/research/analytics/aktualnye-kiberugrozy-na-blizhnem-vostoke-2023-2024/ (дата обращения: 04.03.2025).
[19] Там же.

Главными последствиями кибератак хактивистов и APT-группировки – нарушение деятельности компаний и утечка данных, где злоумышленников преимущественно интересует получение денежной выгоды. Реализация недопустимых событий для банков, страховых и инвесткомпаний, криптовалютных бирж приводит к денежному ущербу, потере клиентов (график 7).

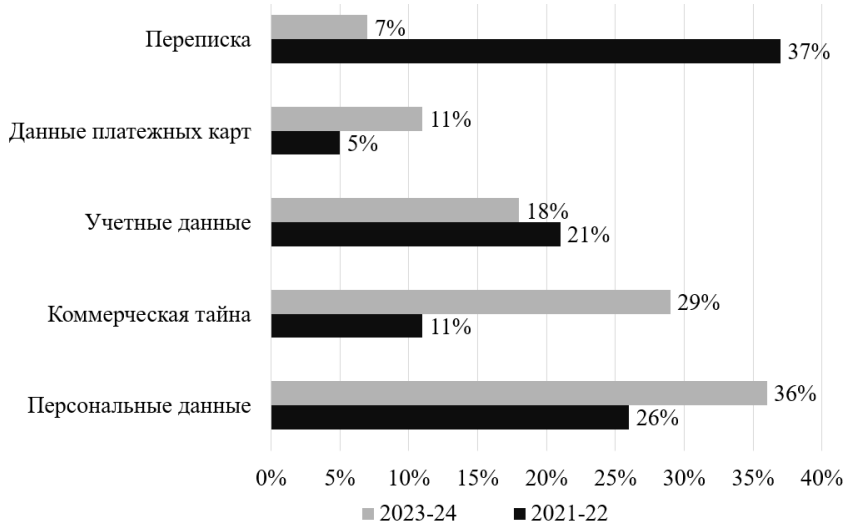

График 7. Виды утекших данных, ИРИ, %, 2021–2024 гг.[20]

Из иранских организаций наиболее часто атакам подвергаются госучреждения, на которые пришлось треть атак киберпреступников в 2021–2022 гг. и 35% – в 2023 – первом полугодии 2024 г., когда 24% всех кибератак пришлось на финансовые организации страны. Для сравнения: в России 64% кибератак в 2024 г. пришлось на компании критической информационной инфраструктуры[21]. Телекоммуникационная инфраструктура Ирана также страдает от действий киберпреступников. Например, в 2023 г. злоумышленники атаковали иранского мобильного оператора, остановившего предоставление услуг связи на 12 часов, что нарушило работу интернета во всем Иране. Кибератаки на промышленные пред-

[20] Ландшафт киберугроз в Иране: 2021 – H1 2024 // Позитивные Технологии. – 29.10.2024. – URL: https://www.ptsecurity.com/ru-ru/research/analytics/landshaft-kiberugroz-v-irane-2021-h1-2024/ (дата обращения: 02.03.2025).

[21] Российский рынок ИБ и его роль в мировой индустрии: итоги 2024 года и прогнозы на 2025 // Позитивные Технологии. – 18.12.2024. – URL: https://www.ptsecurity.com/ru-ru/research/analytics/rossijskij-rynok-ib-i-ego-rol-v-mirovoj-industrii-itogi-2024-goda-i-prognozy-na-2025/#id2 (дата обращения: 05.03.2025).

приятия злоумышленников нарушают технологические процессы, преступники получают доступ к внутренним системам управления, к данным о сотрудниках и операционной деятельности организаций.

Россия фактически превратилась в мировой киберполигон с февраля 2022 г. и число кибератак на российские компании продолжает расти. За 2024 г. количество атак киберпреступников выросло в 2,5 раза до 130 тыс., где промышленные предприятия остаются самыми атакуемыми. По оценкам ряда экспертов в 2025 г. число успешных кибератак сохранится в диапазоне 5–10%[22]. Российский рынок кибербезопасности в 2024 г. вырос до ~593,4 млрд руб., сохраняя среднегодовые темпы роста в 30% за 2019–2023 гг. В прошлом году почти половина (46%) продаж российского кибербеза была сгенерирована решениями по программному обеспечению, аппаратное обеспечение принесло 19%, на ИТ-услуги пришлось свыше трети рынка (35%)[23]. Напомним, что до 2025 г. российские кредитные организации, как владельцы критической информационной инфраструктуры, должны были перейти на отечественное программное обеспечение с разработанного в «недружественных» странах, согласно указу Президента России В.В. Путина, благодаря чему 2023–2024 гг. стали прорывными для российских разработчиков кибербезрешений. Благодаря импортозамещению в сфере информационной безопасности новые отечественные инструменты позволили более эффективно бороться с киберугрозами.

Тем не менее ожидается, что в 2025 г. отечественный рынок кибербезрешений вырастет только на 10–15%, поэтому российским разработчикам необходим выход на зарубежные рынки[24]. В 2023–2024 гг. российские компании по информационной и кибербезопасности успешно выходили на рынки ближневосточных стран, в том числе и в Иран, предлагая отечественные решения, включая экспертизу в контейнерах и облаках, киберполигоны, позволяющие белым хакерам находить уязвимости и генерировать недопустимые события (на которые ожидается удвоение со стороны корпораций), ИИ-инструменты, машинное обучение, квантовые технологии, межсетевые экраны (для защиты инфраструктуры). В частности, начались отгрузки за рубеж межсетевого экрана нового поколения NGFW (Next Generation Firewall) от российского (публичного) кибербезразработчика «Позитивные технологии». Российские разработчики проводят обучение для заказчиков из (более чем двадцати) «дружественных» стран, также предлагая выездные семинары в Индии, странах Персидского залива.

[22] Число кибератак на российские компании за год выросло в 2,5 раза // Бизнес-секреты. – 14.01.2025. – URL: https://secrets.tbank.ru/novosti/kiberataky-2024/ (дата обращения: 07.03.2025).
[23] Исследование: по итогам 2024 года отечественный рынок информационной безопасности вырастет на 30% // Хабр. – 19.12.2024. – URL: https://habr.com/ru/news/867994/ (дата обращения: 10.03.2025).
[24] Там же.

Существует ряд особенностей при выходе на рынки Ближнего Востока и Африки: 1) ИТ-ландшафт и ИТ-решения кардинально отличаются от российских; 2) русские решения по кибербезопасности впервые появляются на Востоке; 3) отсутствие собственных решений и доминирование американских приводит к тому, что заказчики проявляют огромный интерес к российским альтернативам; 4) наблюдается так называемый «зоопарк» решений, т.е. когда после приобретения ПО заказчики не умеют внедрять и управлять решениями. Существуют и особенности в отдельных странах: 1) наиболее зрелые заказчики отмечены в Малайзии и КСА; 2) в Индии действуют много западных компаний, которые обучают специалистов для себя (Google, ABC, Cisco), несмотря на правительственный запрос «Made in India»; 3) в ОАЭ – высокий спрос на российские аналоги американских решений[25].

По мнению Игоря Ашманова, члена Совета по правам человека при Президенте России, в той или иной степени цифровым суверенитетом в мире обладают только три страны: США обладают полным цифровым суверенитетом, КНР – неполным, а Россия – еще более неполной степенью цифровой суверенности[26]. Как полагает эксперт, «цифровая колонизация» со стороны зарубежных технологических держав – основная угроза для России[27]. Пришедшие в СССР в конце 1980-х – начале 1990-х годов американские цифровые техгиганты, по большей части уничтожили зарождающийся отечественный ИТ-рынок и компьютерную отрасль (во многом коррупционным путем). Выжило ограниченное количество отечественных ИТ-компаний, в основном те, которым помогало государство заказами или путем регулирования: 1С (бухгалтерские решения и ERP), Лаборатория Касперского (антивирусы), Яндекс (поисковик) и т.п. Отечественные аппаратные производители были практически уничтожены. Напротив, системные интеграторы, дистрибуторы (т.е. импортеры, продавцы западных компьютеров, серверов) доминировали на российском ИТ-рынке в 1990–2010-е годы, как и оффшорные аутсоринговые компании, среди клиентов которых были западные компании, пришедшие в Россию (Boeing, Deutsche Bank, Reuters).

На сегодняшний день Россия достигла полной самообеспеченности по ключевым показателям устойчивости. Сюда относятся энергетика, при-

[25] Лаврова Д. Индия: ландшафт киберугроз Q3 2023 – Q3 2024 // Позитивные Технологии. – 22.10.2024. – URL: https://www.ptsecurity.com/ru-ru/research/analytics/indiya-landshaft-kiberugroz-q3-2023-q3-2024/#id1 (дата обращения: 02.02.2025).

[26] «Мы – во многом колония США»: Ашманов объяснил на примерах, что такое цифровой суверенитет // Царьград ТВ. – 22.10.2021. – URL: https://tsargrad.tv/news/my-vo-mnogom-kolonija-ssha-ashmanov-objasnil-na-primerah-chto-takoe-cifrovoj-suverenitet_435383 (дата обращения: 20.05.2025).

[27] Игорь Ашманов: главная угроза для России не кибератаки, а цифровая колонизация // Бизнесonline. – 14.05.2025. – URL: https://www.business-gazeta.ru/news/672194 (дата обращения: 20.05.2025).

родные ресурсы, развитая инфраструктура (трубопроводы, железные дороги, порты), инвестиции в технологии (включая разработку, извлечение и переработку труднодоступных месторождений), образование, ВПК, армия, военные технологии, военная и гражданская авиация, микроэлектроника, биотехнологии, лазеры и квантовые технологии, производство компьютеров и электроники, транспортное машиностроение, атомная энергетика, судостроение, продовольственная независимость, цифровизация и модернизация сферы здравоохранения, формирующая мировые тренды в математике, физике, инженерии, биологии российская наука.

Контрактные производства, которыми российские компании пользовались для производства своей продукции тридцать лет, сейчас строятся внутри России, и уже отечественные заводы могут принимать заказы на контрактное производство для иностранных брендов, в первую очередь тех, кто собирается работать на территории России. Контрактное производство электроники в РФ в 2023 г. выросло на 42% до 35 млрд руб., а рост производства компьютеров, электронных и оптических изделий в первом квартале 2024 г. составил 42,4% по сравнению с первым кварталом 2023 г.[28]

В 2023–2024 гг. в российской микроэлектронике начался новый этап углубления импортозамещения, когда вместо брендирования китайских товаров и крупноузловой сборки из готовых печатных плат развивается пайка печатных плат, так называемый поверхностный монтаж. На очереди следующий этап импортозамещения оборудования, сырья и электронно-компонентной базы (транзисторов, конденсаторов, резисторов, микросхем и т.п.) для гражданской инфраструктуры, которые пока реализуются на заводах ВПК и на стратегически важных инфраструктурных объектах.

Таким образом, Россия может предложить Ирану как отечественные решения по кибербезопасности, так и другие технологии, в частности по микроэлектронике. В марте 2025 г. Зеленоградский нанотехнологический центр и Штаб по развитию нано- и микротехнологий Исламской Республики Иран подписали меморандум о сотрудничестве в сфере развития радиоэлектронной промышленности, включая производство литографического оборудования для печати чипов, телекоммуникационных мультиплексоров, датчиков для автомобилей, пр., где ЗНТЦ будет выступать как интегратор контрактных производств для ИРИ[29].

У российских технологических компаний есть опыт работы в странах Азии. В частности, в 2007–2015 гг. российский публичный холдинг «АФК Система» предоставлял услуги связи в Индии через свою дочернюю

[28] Российский рынок контрактного производства электроники вырос в 1,5 раза // Ведомости. – 25.04.2024. – URL: https://www.vedomosti.ru/technology/articles/2024/04/25/1034009-rossiiskii-rinok-kontraktnogo-proizvodstva-elektroniki-viros (дата обращения: 09.03.2025).

[29] Чипы с персидским отливом // Коммерсант. – 10.03.2025. – URL: https://www.kommersant.ru/doc/7563596?ysclid=m91xboo82e270986018 (дата обращения: 10.03.2025).

компанию мобильного оператора Sistema Shyam Teleservices, а в 2018 г. совместно с Ru-Net Holdings вложил $5 млн долл. в Faaso's (egrocery) в 2018 г.[30] Это индийская онлайн-платформа Faaso's, занимающаяся приготовлением и доставкой еды, владевшая на тот момент 170 кухнями в 15 индийских городах, а также управлявшая несколькими ресторанными брендами. Также в 2018 г. венчурный фонд АФК «Система» и государственная инвесткомпания Сингапура Temasek Holdings вложили 30 млн долл. в индийскую платформу в сфере потребительского кредитования Kissht. Основанная в 2015 г. Kissht на момент сделки сотрудничала с 3 тыс. оффлайн магазинами в Индии и с более чем с 50 онлайн-магазинами (разработав самообучающийся алгоритм по оценке кредитного профиля клиента за 90–120 секунд на основе более чем двух тысяч параметров)[31]. В 2024 г. публичная ведущая российская ИТ-компания «Софтлайн» приобрела за 50 млн долл. индийского системного интегратора[32]. И тогда же популярная российская сеть магазинов Fix Price начала пробовать свой формат в ОАЭ, после обкатки которой может выйти в Индию.

Примерами развивающегося технологического сотрудничества между Россией и Ираном могут послужить как исторический опыт, так и недавние двусторонние инициативы. Иран и Россия имеют давнюю историю сотрудничества в горнодобывающем секторе, что привело к запуску высокопроизводительных шахт в Иране, а в 1961 г. специалисты Советского Союза построили первое предприятие тяжелой промышленности в Иране – металлургический комбинат Мобареке в Исфахане. Россия оказалась единственной страной, обладавшей политической волей и соответствующими атомными технологиями, чтобы силами «Росатома» построить в 1995–2011 гг. АЭС «Бушер», выполнив при этом главное пожелание иранской стороны – достройку 1-го блока (построить который с нуля было бы проще и дешевле в силу отсутствия конструкторской документации, пробитого авиабомбой купола реакторного здания, и т.п.). По оценкам Хуссейна Гаффари, директора АЭС «Бушер», к концу октября 2017 г., построенный российскими специалистами 1-й блок АЭС «Бушер» сэкономил стране 6,1 млрд барр. сырой нефти на 2 млрд долл.[33]

---

[30] АФК «Система» инвестировала в индийский сервис доставки еды // Ведомости. – 03.08.2018. – URL: https://www.vedomosti.ru/business/articles/2018/08/03/777289-sistema-dostavki-edi (дата обращения: 11.03.2025).

[31] Фонд АФК «Система» и другие инвестировали $30 млн в индийскую платформу кредитования Kissht // Русбейс. – 14.09.2018. – https://rb.ru/news/afk-sistema-kissht/?ysclid=m91xguhtab488536102 (дата обращения: 09.03.2025).

[32] «Софтлайн» планирует приобрести системного интегратора в Индии // Интерфакс. – 16.05.2024. – URL: https://www.interfax.ru/business/960851 (дата обращения: 06.03.2025).

[33] АЭС Бушер сэкономила Ирану 2,54 млрд долл США // Neftea.ru. – 07.11.2018. – URL: https://neftegaz.ru/news/nuclear/197238-aes-busher-v-sekonomila-iranu-2-54-mlrd-doll-ssha/ (дата обращения: 10.03.2025).

Иран разрабатывает и свои собственные технологии. В марте 2025 г. компания по горнодобывающей и металлургической промышленности Ирана, исполнительный орган Организации по развитию и реконструкции шахт и горнодобывающей промышленности Ирана (IMIDRO), разработала собственную технологию производства губчатого железа PERED (Persian Reduction) и подписала соглашение о сотрудничестве с крупными китайскими производителями стали[34]. А ранее, в феврале 2025 г. глава Организации по развитию и реконструкции шахт и горнодобывающей промышленности Ирана Мохаммад Агаджанлоу на встрече с российской горнодобывающей компанией «Зарубежгеология» заявил, что Иран и Россия намерены создать совместный комитет для надзора за реализацией соглашения о сотрудничестве в горнодобывающей промышленности, отметив, что иранская технология прямого восстановления PERED стала конкурентом процесса MIDREX и может использоваться российскими компаниями[35]. Помимо этого, в 2025 г. в Иране планируется запустить первую нефтяную скважину, оборудованную искусственным интеллектом (ИИ), на нефтяных месторождениях Сепер и Джофейр, а также готовится запуск первого в стране «интеллектуального» НПЗ на о. Кешм.

Однако из-за вынужденной международной изоляции в Иране нет многих гражданских и военных технологий. Отчасти поэтому в августе 2024 г. Министерство промышленности, горнодобывающей промышленности и торговли Ирана разработало комплекс поддержки для содействия экспорту наукоемких и инновационных продуктов, включающий скидки на импортные и экспортные пошлины на продукцию, приоритет импорта сырья и оборудования, необходимого поддерживаемым компаниям, упрощение юридических и административных процессов, связанных с экспортом и импортом, консалтинг. Закон о поддержке компаний и учреждений, основанных на знаниях, и коммерциализации инноваций и изобретений был одобрен иранским парламентом в 1389 г. (по иранскому календарю, по григорианскому календарю – 2010–2011 гг.), что способствовало удвоению количества наукоемких компаний с 6,474 летом 2021 г. до 9,215 в 2023 г., и увеличению занятого там персонала в 8,4 раза до 420 тыс. человек[36]. Кроме того, начиная с 2000 г. Министерство науки, исследований и технологий Ирана проводит ежегодную «Неделю исследований и технологий», основные задачи которой – привлечь внимание обществен-

[34] MME signs co-op agreement with leading Chinese steelmakers // Tehran Times. – 11.03.2025. – URL: https://www.tehrantimes.com/news/510801/MME-signs-co-op-agreement-with-leading-Chinese-steelmakers (дата обращения: 16.03.2025).

[35] Tehran, Moscow to expand mining cooperation // Tehran Times. – 24.02.2025. – URL: https://www.tehrantimes.com/news/510151/Tehran-Moscow-to-expand-mining-cooperation (дата обращения: 17.03.2025).

[36] Industry Ministry unveils export support package for knowledge-based firms // Tehran Times. – 27.08.2024. – URL: https://tehrantimes.com/news/502976/Industry-Ministry-unveils-export-support-package-for-knowledge-based (дата обращения: 15.03.2025).

ности к науке и технологиям Ирана, развитие технологий и исследований в стране, поддержка иранских ученых, а также популяризация технологий в иранском обществе.

* * *

Вследствие вынужденной международной изоляции ИРИ уровень решений по защите инфраструктуры информационной безопасности в стране остается недостаточно высоким. В связи с этим Ирану необходимо создавать собственные функциональные программно-аппаратные решения для развития устойчивости собственной инфраструктуры к кибератакам.

На сегодняшний день Россия достигла полной самообеспеченности по ключевым показателям устойчивости, у российских технологических компаний есть опыт работы в странах Азии, поэтому Россия может предложить Ирану как отечественные решения по кибербезопасности, так и другие технологии, в частности по микроэлектронике. Для России сотрудничество с Ираном в сфере технологий имеет большое значение как с точки зрения выхода на рынки «дружественных» стран в условиях формирования нового миропорядка, так и с точки зрения монетизации российских разработок на быстрорастущем рынке, каким является ИРИ.

Список источников и литературы

1. Актуальные киберугрозы на Ближнем Востоке: 2023–2024 // Позитивные Технологии. – 18.10.2024. – URL: https://www.ptsecurity.com/ru-ru/research/analytics/aktualnye-kiberugrozy-na-blizhnem-vostoke-2023-2024/ (дата обращения: 04.03.2025).
2. АФК «Система» инвестировала в индийский сервис доставки еды // Ведомости. – 03.08.2018. – URL: https://www.vedomosti.ru/business/articles/2018/08/03/777289-sistema-dostavki-edi (дата обращения: 11.03.2025).
3. АЭС Бушер сэкономила Ирану 2,54 млрд долл. США // Neftea.ru. – 07.11.2018. – URL: https://neftegaz.ru/news/nuclear/197238-aes-busher-v-sekonomila-iranu-2-54-mlrd-doll-ssha/ (дата обращения: 10.03.2025).
4. Игорь Ашманов: главная угроза для России не кибератаки, а цифровая колонизация // Бизнесonline. – 14.05.2025. – URL: https://www.business-gazeta.ru/news/672194?ysclid=max0kjyy7413982289 (дата обращения: 20.05.2025).
5. Иран улучшил позиции в Глобальном индексе готовности правительств к искусственному интеллекту // Информационное агентство Исламской Республики (ИРНА). – 24.02.2025. – URL: https://ru.irna.ir/news/85761070/Иран-Улучшил-Позиции-в-Глобальном-Индексе-Готовности-Правительств (дата обращения: 20.05.2025).

6. Исследование: по итогам 2024 года отечественный рынок информационной безопасности вырастет на 30% // Хабр. – 19.12.2024. – URL: https://habr.com/ru/news/867994/ (дата обращения: 10.03.2025).
7. Лаврова Д. Индия: ландшафт киберугроз Q3 2023 – Q3 2024 // Позитивные Технологии. – 22.10.2024. – URL: https://www.ptsecurity.com/ru-ru/research/analytics/indiya-landshaft-kiberugroz-q3-2023-q3-2024/#id1 (дата обращения: 02.02.2025).
8. Ландшафт киберугроз в Иране: 2021 – H1 2024 // Позитивные Технологии. – 29.10.2024. – URL: https://www.ptsecurity.com/ru-ru/research/analytics/landshaft-kiberugroz-v-irane-2021-h1-2024/ (дата обращения: 02.03.2025).
9. «Мы – во многом колония США»: Ашманов объяснил на примерах, что такое цифровой суверенитет // Царьград ТВ. – 22.10.2021. – URL: https://tsargrad.tv/news/my-vo-mnogom-kolonija-ssha-ashmanov-objasnil-na-primerah-chto-takoe-cifrovoj-suverenitet_435383 (дата обращения: 20.05.2025).
10. Российский рынок ИБ и его роль в мировой индустрии: итоги 2024 года и прогнозы на 2025 // Позитивные Технологии. – 18.12.2024. – URL: https://www.ptsecurity.com/ru-ru/research/analytics/rossijskij-rynok-ib-i-ego-rol-v-mirovoj-industrii-itogi-2024-goda-i-prognozy-na-2025/#id2 (дата обращения: 05.03.2025).
11. Российский рынок контрактного производства электроники вырос в 1,5 раза // Ведомости. – 25.04.2025. – URL: https://www.vedomosti.ru/technology/articles/2024/04/25/1034009-rossiiskii-rinok-kontraktnogo-proizvodstva-elektroniki-viros (дата обращения: 09.03.2025).
12. «Софтлайн» планирует приобрести системного интегратора в Индии // Интерфакс. – 16.05.2024. – URL: https://www.interfax.ru/business/960851 (дата обращения: 06.03.2025).
13. Фонд АФК «Система» и другие инвестировали $30 млн в индийскую платформу кредитования Kissht // Русбейс. – 14.09.2018. – https://rb.ru/news/afk-sistema-kissht/ (дата обращения: 09.03.2025).
14. Чипы с персидским отливом // Комерсант. – 10.03.2025. – URL: https://www.kommersant.ru/doc/7563596 (дата обращения: 10.03.2025).
15. Число кибератак на российские компании за год выросло в 2,5 раза // Бизнес-секреты. – 14.01.2025. – URL: https://secrets.tbank.ru/novosti/kiberataky-2024/ (дата обращения: 07.03.2025).
16. Чурсина А. Страны Персидского залива как товар на рынке преступных киберуслуг (анализ 2023–2024 годов) // Позитивные Технологии. – 18.09.2024. – URL: https://www.ptsecurity.com/ru-ru/research/analytics/gulf-countries-as-a-commodity-in-the-market-on-criminal-cyber-services-2023-2024/#id1 (дата обращения: 01.03.2025).
17. Economic Trends // Central Bank of the Islamic Republic of Iran. – URL: https://cbi.ir/category/EconomicTrends_en.aspx (дата обращения: 15.03.2025).
18. Industry Ministry unveils export support package for knowledge-based firms // Tehran Times. – 27.08.2024. – URL: https://tehrantimes.com/news/502976/Industry-Ministry-unveils-export-support-package-for-knowledge-based (дата обращения: 15.03.2025).

19. Iran GDP Annual Growth Rate // Trading economics. – URL: https://tradingeconomics.com/iran/gdp-growth-annual (дата обращения: 10.03.2025).
20. Iran needs $200 b of investment by 2031 to achieve economic goals' // Tehran Times. – 12.10.2024. – URL: https://tehrantimes.com/news/504858/Iran-needs-200b-of-investment-by-2031-to-achieve-economic-goals (дата обращения: 16.03.2025).
21. Iran needs $4 b to expand maritime fleet: IDRO // Tehran Times. – 11.02.2025. – URL: https://www.tehrantimes.com/news/509633/Iran-needs-4b-to-expand-maritime-fleet-IDRO (дата обращения: 14.03.2025).
22. Iran signs $17 b deal to boost gas pressure at South Pars field // Tehran Times. – 08.03.2025. – URL: https://www.tehrantimes.com/news/510663/Iran-signs-17b-deal-to-boost-gas-pressure-at-South-Pars-field (дата обращения: 17.03.2025).
23. MME signs co-op agreement with leading Chinese steelmakers // Tehran Times. – 11.03.2025. – URL: https://www.tehrantimes.com/news/510801/MME-signs-co-op-agreement-with-leading-Chinese-steelmakers (дата обращения: 16.03.2025).
24. Tehran, Moscow to expand mining cooperation // Tehran Times. – 24.02.2025. – URL: https://www.tehrantimes.com/news/510151/Tehran-Moscow-to-expand-mining-cooperation (дата обращения: 17.03.2025).
25. World Economic Outlook Database: October 2024 Edition // IMF. – URL: https://www.imf.org/en/Publications/WEO/weo-database/2024/October (дата обращения: 14.03.2025).