НАЦИОНАЛЬНАЯ АССОЦИАЦИЯ МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

СБОРНИК МАТЕРИАЛОВ ПО ПРОБЛЕМАТИКЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ГОСУДАРСТВ-ЧЛЕНОВ ЛИГИ АРАБСКИХ ГОСУДАРСТВ

НАЦИОНАЛЬНАЯ АССОЦИАЦИЯ МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

СБОРНИК МАТЕРИАЛОВ ПО ПРОБЛЕМАТИКЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ГОСУДАРСТВ-ЧЛЕНОВ ЛИГИ АРАБСКИХ ГОСУДАРСТВ

МОСКВА – 2023

Коллектив разработчиков:
С.В. Коротков, к.в.н., член-корреспондент Российской инженерной академии, начальник отдела НАМИБ
К.С. Бойко, эксперт НАМИБ
С.Г. Волкова, эксперт НАМИБ
Е.Э. Осечкин, эксперт НАМИБ
А.Г. Цветкова, старший эксперт НАМИБ

Сборник материалов разработан в рамках подготовки к первому Российско-Арабскому Диалогу по международной информационной безопасности (МИБ).

Целью труда является систематизация и обобщение сведений о деятельности Лиги арабских государств и ее государств-членов в сфере противодействия угрозам информационной безопасности в информационном пространстве и продвигаемых национальных, региональных и глобальных инициативах в области МИБ.

Результаты проведенного анализа дают возможность определить основные направления российско-арабского сотрудничества в области МИБ и оценить перспективы их реализации, в том числе, по линии государственно-частного партнерства, а также повысить эффективность взаимодействия с иностранными государствами в интересах совместного противодействия вызовам и угрозам в глобальном информационном пространстве.

Представленные материалы предназначены для профильных структур органов государственной власти, бизнес-сообщества, научных работников, экспертов, специалистов и студентов ВУЗов, занимающихся проблемами обеспечения информационной безопасности и международного сотрудничества в данной области.

Материалы подготовлены в соответствии с уставными задачами НАМИБ по выпуску материалов по вопросам реализации основных направлений государственной политики в области МИБ.

Содержание

I. Общие сведения о Лиге арабских государств (ЛАГ)

История создания: Создана 22 марта 1945 г. на основании Александрийского протокола. Штаб-квартира Лиги находится в Каире (Египет).

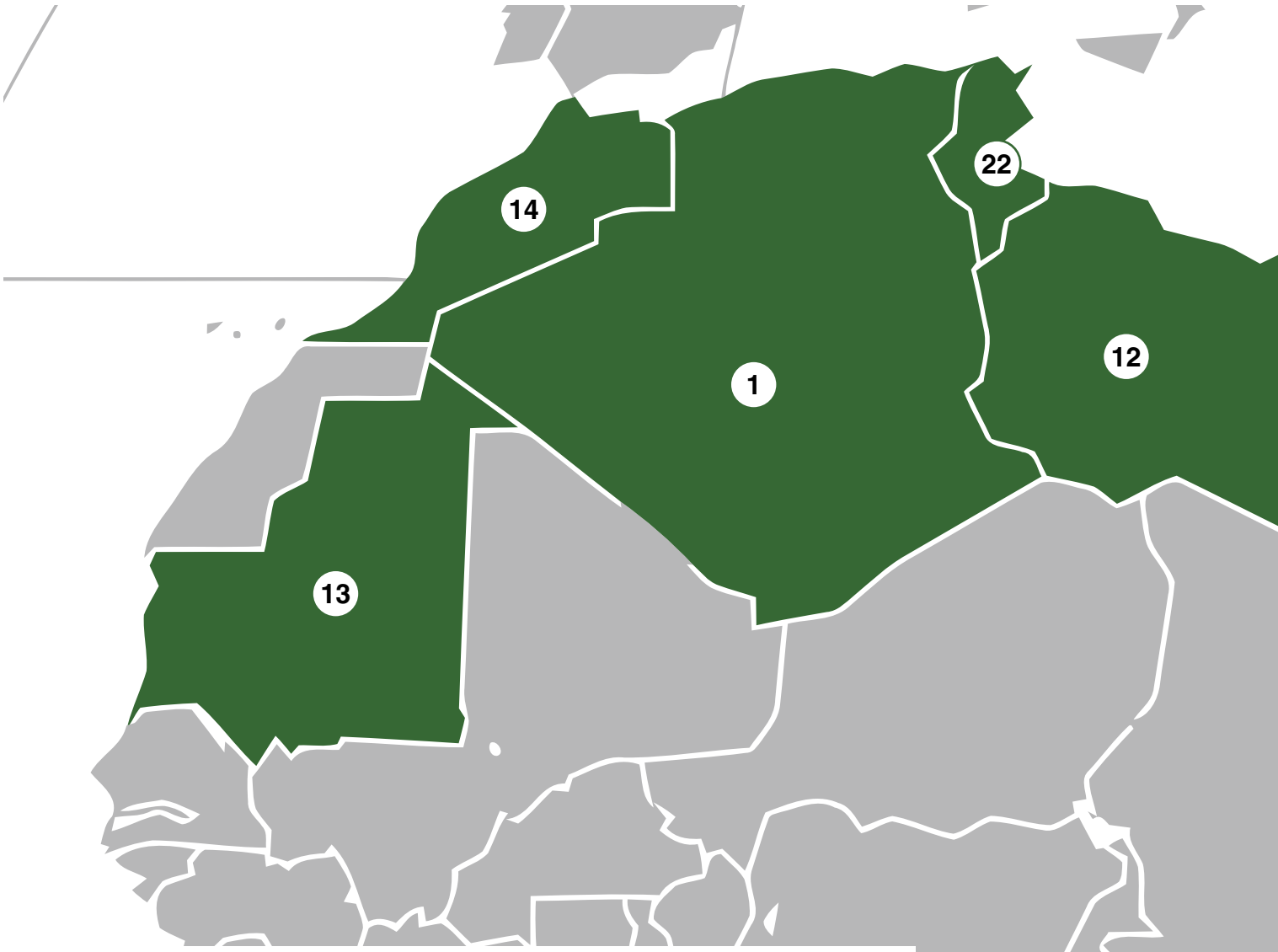
Официальный язык: арабский.

Цели: Цели Лиги определены в соглашении, подписанном в 1945 году, и предусматривают «укрепление связей между государствами, участвующими в ней, выработку единой политической линии для осуществления сотрудничества между ними, защиты их независимости и суверенитета, для рассмотрения дел и интересов арабских стран». Сотрудничество не ограничивается политическими аспектами и включает также экономические, финансовые, коммуникационные, культурные, социальные и санитарные взаимодействия. Кроме того, сотрудничество включает вопросы подданства, паспортов, виз, выдачи преступников.

Государства-члены: Алжир, Бахрейн, Джибути, Египет, Иордания, Ирак, Йемен, Катар, Коморы, Кувейт, Ливан, Ливия, Мавритания, Марокко, ОАЭ, Оман, Палестина, Саудовская Аравия, Сирия (членство приостановлено 16 ноября 2011 г.), Сомали, Судан, Тунис.

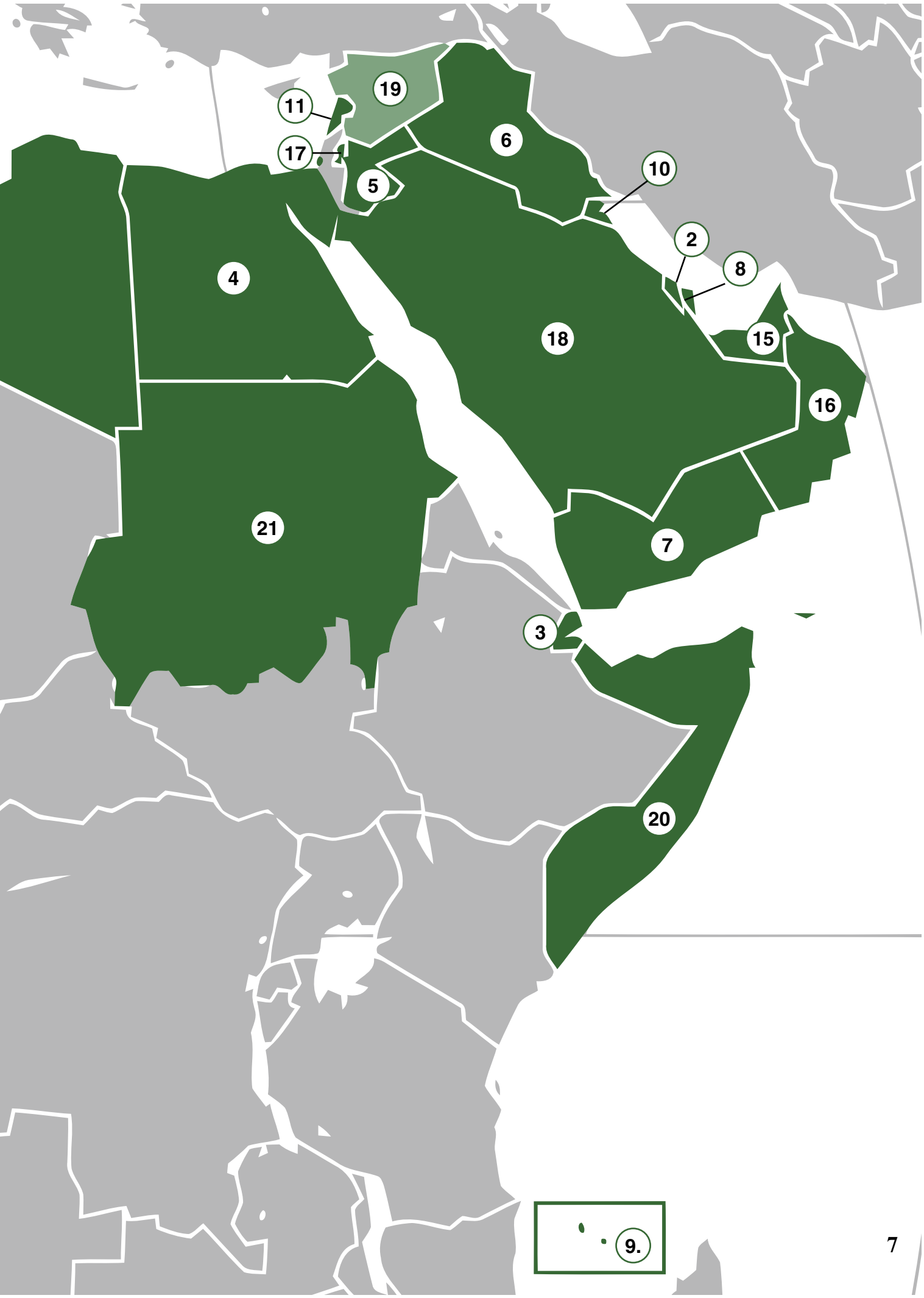
Основные руководящие органы: Высшим руководящим органом организации является Совет Лиги. Каждый член имеет в Совете один голос, обычно страну представляет министр иностранных дел или постоянный представитель в Совете, который собирается дважды в год, в марте и сентябре. При ходатайстве по крайней мере двух стран, может быть собрана внеочередная сессия Совета. Решения, принимаемые Советом Лиги, обязательны к исполнению теми странами, которые голосовали за них.

В период между сессиями Совета руководство осуществляется Генеральным секретариатом, во главе которого стоит генеральный секретарь, избираемый сроком на пять лет. Помимо этого, в Лиге работают экономический совет, объединённый комитет обороны и другие постоянные комитеты (экономический,



Список государств-членов Лиги арабских государств

1. Алжирская Народная Демократическая Республика
2. Королевство Бахрейн
3. Республика Джибути
4. Арабская Республика Египет
5. Иорданское Хашимитское Королевство
6. Республика Ирак
7. Йеменская Республика
8. Государство Катар
9. Союз Коморских Островов
10. Государство Кувейт
11. Ливанская Республика
12. Государство Ливия
13. Исламская Республика Мавритания
14. Королевство Марокко
15. Объединенные Арабские Эмираты
16. Султанат Оман
17. Государство Палестина
18. Королевство Саудовская Аравия
19. Сирийская Арабская Республика (членство приостановлено)
20. Федеративная Республика Сомали
21. Республика Судан
22. Тунисская Республика


19
11
17
6
5
10
2
8
4
18
15
16
21
7
3
20
9.

транспортный, по здравоохранению, по законодательству, по культуре, по социальным вопросам).

Территория: Государства-члены занимают общую площадь 5,25 млн кв. миль.

Население: В государствах-членах Лиги проживает более 500 млн человек.

Представительство Лиги арабских государств в России расположено по адресу: г. Москва, Трубниковский переулок, дом 23, строение 1.

II. Основные особенности политики Лиги арабских государств в области региональной и международной информационной безопасности

1. Факторы, определяющие задачи региональной политики кибербезопасности

В условиях набирающей обороты цифровизации разработка региональной политики кибербезопасности стала уникальной повесткой, которая смогла объединить интересы всех государств-членов Лиги арабских государств (ЛАГ). Совокупность следующих факторов определила этот важный политический процесс и направления сотрудничества в сфере кибербезопасности и формирования системы международной информационной безопасности (МИБ).

1. Цифровизация является новой точкой роста экономики и социального развития ЛАГ, что способствует улучшению качества жизни и реализации целей устойчивого развития ООН (резолюция Генеральной Ассамблеи ООН A/RES/70/1 от 25 сентября 2015 г. «Преобразование нашего мира: Повестка дня в области устойчивого развития на период до 2030 года»). Однако стремительный рост информатизации стран Персидского залива усугубляет «цифровой разрыв» с бедными странами региона и сокращает возможные выгоды Индустрии 4.0. «Возможность доступного, недорогого и надежного подключения, особенно к широкополосному Интернету, играет решающую роль в обеспечении перехода на цифровые технологии».

2. При этом уровень развития внутри региональной ИКТ инфраструктуры низкий, наличие 28 точек обмена международным трафиком (IXPs) является недостаточным показателем. Настоятельно требуется скоординированная с международным союзом электросвязи (МСЭ) политика в технологической сфере.

3. Уровень преступности с использованием ИКТ в регионе очень высокий. Он отражает острый конфликт геополитических и экономических интересов отдельных государств Ближнего Востока и Северной Африки, а также высокую привлекательность для компьютерных атак информационных систем «богатых» стран Персидского залива. В регионе отмечается весь спектр вредоносной и злонамеренной деятельности: использование киберпространства для воздействия на общественное сознание, в частности в террористических целях; хакерские атаки с разной мотивировкой; компьютерные преступления; наступательные кибероперации, осуществляемые государственными акторами различных стран. Компьютерные атаки осуществляются ежедневно, по сути кибервойна стала нормой жизни на Ближнем Востоке.

4. Потери от компьютерных атак наносят серьезный экономический урон. Например, Саудовская Аравия в 2020 году подверглась более, чем 22,5 млн компью-

терных атак, каждая из которых обошлась государству в $6,5 млн, а в условиях пандемии COVID-19 только в первом квартале 2021 года их стоимость возросла до $7 млн. По данным 2020 года американского института Ponemon Institute, средняя стоимость утечки данных в результате киберинцидентов в среднем обошлась компаниям Ближнего Востока в $6,53 млн. Кроме того, свойственные населению Ближнего Востока пассионарность и религиозный фанатизм создают условия для проведения против потенциальных противников компьютерных атак с деструктивным эффектом. В этих обстоятельствах снижение цифровых угроз становится интегральной частью финансовой безопасности и экономической стабильности.

5. На данный момент для развития ИКТ инфраструктуры и обеспечения ее безопасности государства-члены ЛАГ испытывают значительную технологическую и кадровую зависимость от индустриально развитых стран. К импортным технологиям (из США, КНР, Израиля и России) в регионе относятся с осторожностью, одной из главных угроз практически все государства считают инсайдерскую деятельность. В связи с этим при информатизации госсектора предпочтение отдается программному обеспечению с открытым программным кодом (в первую очередь такой стратегии придерживаются Египет, Иордания, Катар, ОАЭ, Оман, Саудовская Аравия и Тунис). Но и в частном секторе государства региона хотят иметь гарантии безопасности и предпочитают совместные разработки или получение технологий.

6. Стимулирующим фактором повышения региональной кибербезопасности является скоординированная политика по подготовке собственных кадров, долю которых в частном секторе планируется довести до 50%. Арабская стратегия по научно-техническим исследованиям и инновациям в 2014 году поставила задачу повышения университетского научного образования и увеличения научно-технической деятельности. Параллельно с этим развиваются программы просветительской деятельности по повышению культуры информационной безопасности всех уровней пользователей.

7. Для наиболее развитых стран региона безопасность и стабильность цифровой инфраструктуры высокотехнологичного производства жизненно важна: нефтегазовая отрасль Саудовской Аравии дает 87% ВВП, в Катаре — 60%, Кувейте — 40%, в ОАЭ — 30%. Наличие большого количества объектов критической инфраструктуры, прежде всего нефтегазовой отрасли, создает серьезные риски для населения (в сентябре 2019 г. осуществлена атака беспилотных дронов на нефтеперерабатывающие предприятия национальной нефтяной компании Саудовской Аравии Saudi Aramco в саудовских городах Абкайк и Хурайс). Решение вопросов безопасности такой инфраструктуры требует повышенного внимания.

8. Кроме того, под влиянием событий «арабской весны» и разоблачения фактов политического шпионажа, государствами-членами ЛАГ переосмыслена роль ИКТ в обеспечении национальной безопасности, в том числе, в сохранении культурных

и религиозных ценностей. Национальные нормативные базы были доработаны для противодействия этой угрозе, но между ними имеются существенные расхождения в подходах и толковании даже взаимно согласованных принципов. Многие государства региона имеют авторитарные формы правления, поэтому вопросы национальной безопасности имеют приоритет над правами человека (в экстренных ситуациях осуществляется прекращение доступа к сети Интернет, социальным медиа и незаконному контенту, осуществляется наблюдение за пользователями. Размещение фейковых новостей в государствах-членах ЛАГ и раньше было ограничено, а в настоящее время носит единичный характер, поскольку большинство СМИ подконтрольно правительствам).

9. Для повышения безопасности регионального киберпространства требуется дальнейшее развитие и гармонизация деятельности групп реагирования на компьютерные инциденты CERT/CSIRT. Такие национальные группы реагирования созданы в 18 государствах-членах ЛАГ (см. Таблицу 1 стр. 30) и выполняют функции единых точек обмена информацией, в частности в интересах международного сотрудничества. Для их взаимодействия создана технологическая платформа — Арабский региональный центр безопасности (ITU-ARCC), осуществляется интеграция Лиги в международную сеть групп реагирования.

10. Географическое положение позволяет ЛАГ влиять на топологию межконтинентальных подводных кабелей, которые обеспечивают связность важнейшей магистрали Азия-Европа (в январе 2020 г. разрыв в Йемене подводного кабеля Falcon привел к сокращению на 80% пропускной способности глобальной сети. Слабоинформатизированную экономику страны этот инцидент не слишком затронул, но соседям — Кувейту и Саудовской Аравии он создал серьезные проблемы на несколько суток. Аналогичные аварии случались неоднократно в Египте, Кувейте и других странах).

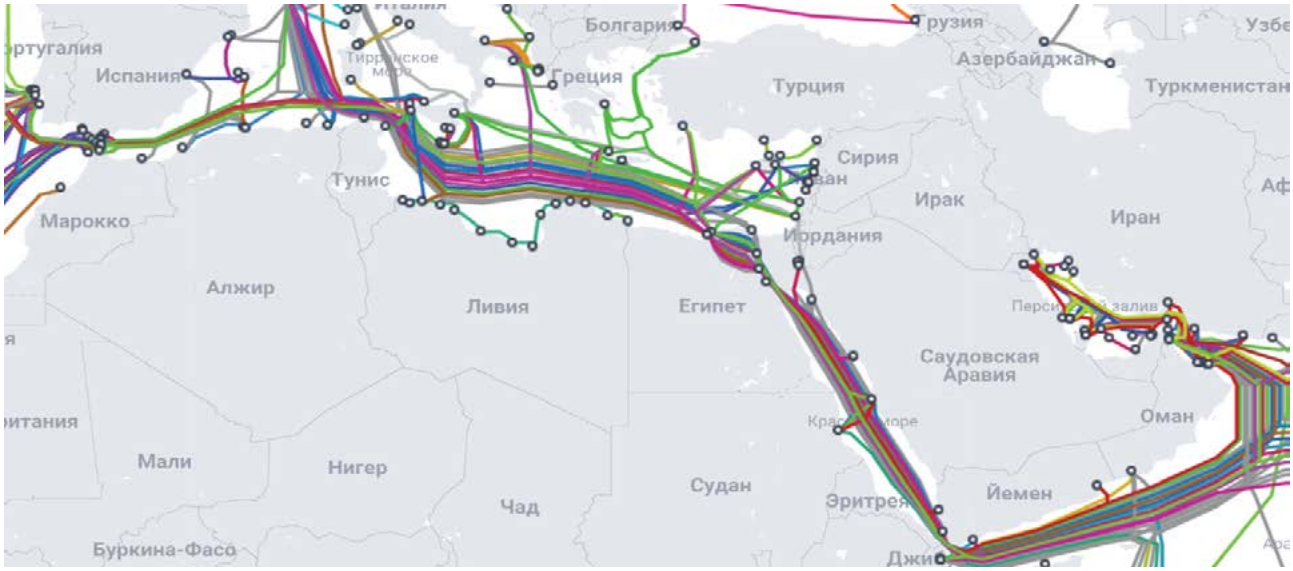


Схема 1. Топология системы подводных кабелей Азия–Европа.
Источник: Submarine Cable Map, https://www.submarinecablemap.com/

Таким образом, ЛАГ может быть одним из основных игроков в выработке политики обеспечения безопасности подводных кабелей.

11. Нефтедобывающие страны региона видят в переходе на передовые цифровые технологии возможность диверсифицировать ориентированную на углеводороды экономику. Они рассчитывают войти в мировые лидеры отрасли ИКТ и разработали соответствующие стратегии развития (см. Таблица 1 стр. 30). Основные инвестиции направлены на технологии Индустрии 4.0 и финтех (развитие «умных городов», использование Интернета вещей и робототехники, Больших данных и искусственного интеллекта, блокчейн и криптовалюты). Безопасность передовых технологий является наиболее актуальным вопросом стратегии кибербезопасности. В связи с этим региональный рынок информационной безопасности будет расти опережающими темпами и к 2024 году достигнет уровня $11,4 млрд.

12. В ЛАГ увеличивается интерес к передовым технологиям в контексте киберобороны. Израиль, обладающий одним из самых высоких технологических и научных потенциалов в этой сфере, способствует росту гонки кибервооружений и провоцирует соседние страны на развитие аналогичных возможностей для защиты национальных интересов. На повестке дня стоит формирование политических, нормативных и технических «правил игры», которые будут учитывать интересы основных игроков.

13. Активно развиваются различные электронные услуги, включая образовательные, медицинские, финансовые, программы электронного правительства (см. Таблица 1 стр. 30 и Рисунок 2 стр. 29). Управление ООН по экономическим и социальным вопросам в 2020 году сделало следующие выводы: «Современные подходы к развитию электронного правительства в регионе во многом основываются на социально-экономическом статусе отдельных стран, хотя другие факторы могут также сказываться. Страны, находящиеся в состоянии конфликта или после конфликта, такие как Ирак, Ливия и Йемен, фокусируются, в основном, на улучшении доступа к инфраструктуре ИКТ и базовым государственным услугам. Страны с умеренными уровнями развития, такие как Египет, Иордания и Ливан, улучшают и расширяют свои цифровые предложения, чтобы гарантировать эффективное оказание высококачественных инклюзивных государственных услуг. Страны с более высоким доходом, такие как Бахрейн, Катар и Объединенные Арабские Эмираты, мобилизуют потенциал передовых технологий, чтобы предоставлять продвинутые государственные услуги и гарантировать высокий уровень удовлетворенности пользователей». Все эти программы нуждаются в обеспечении безопасности и скоординированных политиках использования «Больших данных».

14. Несмотря на высокую информатизацию отдельных стран, доля региона среди всех пользователей сети Интернет незначительна — 3,8% (пропорциональна доле в мировом населении). Только если Лига будет выступать единым фронтом, в том числе с участием Сирии и Ливии, то ЛАГ может стать одним

из ведущих игроков в глобальном сотрудничестве в сфере использования ИКТ и обеспечения их безопасности.

Уже сейчас государства региона являются активными участниками глобальных и региональных международных организаций, внося существенный вклад в их работу (см. Рисунок 1 стр. 28).

2. Участие ЛАГ в работе ООН, ее специализированных организаций и форумов по вопросам безопасности ИКТ и международной информационной безопасности (МИБ)

Организацией Объединенных Наций Лига признана в качестве региональной в 1950 году и получила статус наблюдателя. В 1989 году между ЛАГ и ООН был подписан Меморандум о взаимопонимании, действие которого возобновлено в 2016 г. путем заключения протокола о поправках. В июне 2019 г. в Каире ООН открыла отделение связи при ЛАГ. При штаб-квартире организации находится постоянная делегация ЛАГ, что не имеет аналогов и подчеркивает пристальное внимание ООН к региону в контексте глобальной стабильности и безопасности.

Согласно докладу Генерального секретаря ООН (A/73/328 S/2018/592), Лига является важным партнером в деле осуществления Глобальной контртеррористической стратегии (A/RES/60/288), которая включает противодействие использованию Интернета в террористических целях. По причинам того, что в указанной стратегии введено очень узкое определение терроризма, а странами широко применяются законы шариата, государства-члены ЛАГ больше руководствуются Арабской конвенцией противодействия терроризму, которую в 1998 году ратифицировали 16 государств (не присоединились Ирак, Катар, Кувейт, Мавритания, Сомали, Коморы).

Кроме того, статья 15 Арабской конвенции по борьбе с использованием информационных технологий в преступных целях криминализует следующие деяния: распространение и пропаганда идей и принципов террористических групп; финансирование и подготовка террористических операций; облегчение коммуникаций между террористическими организациями; распространение методов работы со взрывчатыми веществами, особенно в целях осуществления террористических операций; распространение религиозного фанатизма и разжигание религиозной розни.

Группа правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности (ГПЭ) и Рабочие группы открытого состава (РГОС)

Процесс широкого международного взаимодействия по снижению угроз неправомерного использования ИКТ и обсуждения проблем формирования систе-

мы обеспечения МИБ на площадке ООН был инициирован Россией в 1998 году (резолюция Генеральной Ассамблеи ООН A/RES/53/70 «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности»).

Впервые ГПЭ по МИБ была созвана в 2004 г. для рассмотрения существующих и потенциальных угроз в сфере информационной безопасности и возможных совместных мер по их устранению, а также для проведения исследования соответствующих международных концепций, которые были бы направлены на укрепление безопасности глобальных информационных и телекоммуникационных систем.

К настоящему моменту состоялось шесть созывов ГПЭ. Состав групп формировался Генеральным секретарем ООН на основе равноправного географического распределения, из ЛАГ участвовали Иордания (2004, 2019), Катар (2009), Египет (2012, 2014, 2016), Марокко (2019). Позиции других государств-членов ЛАГ также принимались ГПЭ во внимание. Так, Катар в 2010 г., а в 2013 г. Иран и Оман официально представили свои материалы к докладу ГПЭ, подчеркнув главенствующую роль ООН в решении рассматриваемых вопросов. Это говорит не только о глубоком понимании в регионе проблем формирования системы обеспечения МИБ, но и желании оказывать влияние на глобальную политику.

Результаты анализа позиций государств-членов ЛАГ при голосовании по наиболее значимым резолюциям Генеральной Ассамблеи ООН по вопросам МИБ (см. Таблицу 2, стр. 31) показывают их высокую заинтересованность в формировании четкого каркаса безопасности на основе норм международного права:

- Девять государств-членов ЛАГ стали соавторами резолюции Генеральной Ассамблеи ООН A/RES/70/237 от 23 декабря 2015 г., включившей в себя нормы ответственного поведения государств, основанные на принципах Устава ООН и других нормах международного права: суверенное равенство; разрешение международных споров мирными средствами таким образом, чтобы не подвергать угрозе международный мир и безопасность и справедливость; отказ в международных отношениях от угрозы силой или ее применения.
- Практически единодушно (за исключением Сомали) 5 декабря 2018 г. был одобрен российский проект резолюции A/RES/73/27 о переформатировании дискуссии по МИБ в прозрачный, инклюзивный диалог и созыве Рабочей группы открытого состава по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности. В отличие от ГПЭ, РГОС – это полноценный орган Генассамблеи ООН, который может вырабатывать и рекомендовать государствам-членам любые документы, вплоть до проектов международных договоров. При этом важно отметить, что против принятия данной ре-

золюции выступили 46 государств, в том числе США, члены ЕС, Канада, Израиль, Австралия и Япония, которые выдвинули свой проект резолюции о продлении работы ГПЭ.

- По итогам работы РГОС, среди участников которой 6% были представители ЛАГ, была принята резолюция A/RES/75/240 от 31 декабря 2020 г., которая продлила проводимую группой работу до 2025 года.
- Американский проект резолюции Генеральной Ассамблеи ООН «Поощрение ответственного поведения государств в киберпространстве в контексте международной безопасности» A/RES/73/266 был принят 22 декабря 2018 г. Из государств-членов ЛАГ против него проголосовали Египет, Коморы и Сирия. В состав ГПЭ, созванный на основе резолюции, были включены Иордания и Марокко. Таким образом два года параллельно существовало два трека (РГОС и ГПЭ) для обсуждения проблем формирования системы обеспечения МИБ. В 2021 году работа ГПЭ была завершена консенсусным докладом A/76/135. Ввиду успешности РГОС ГПЭ не уполномочена выдвигать резолюции работа по тематике МИБ в ООН в формате ГПЭ была прекращена.
- Важна также поддержка в ЛАГ российской инициативы по созданию в Третьем комитете ООН Специального межправительственного комитета экспертов открытого состава для разработки всеобъемлющей международной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях[1]. Воздержались при голосовании по ней лишь Марокко и Тунис, присоединившиеся к Будапештской конвенции по киберпреступности, Джибути, а также проамерикански настроенные Саудовская Аравия и Бахрейн.

Оценивая активность ЛАГ в различных форматах работы по проблематике МИБ, следует отметить, что несколько стран (Кувейт, Ливан, Марокко, Катар, Тунис и ОАЭ) поддержали в 2018 году. Парижский призыв к доверию и безопасности в киберпространстве, обходящий центральную роль ООН в этом вопросе.

Международный союз электросвязи (МСЭ)

Лига арабских государств принимает все более активное участие в работе МСЭ.

На основании решения Всемирной ассамблеи по стандартизации электросвязи в 2016 году в рамках исследовательских комиссий Сектора стандартизации (МСЭ-Т) созданы региональные группы. Региональная группа ЛАГ работает

1 Резолюция Генеральной Ассамблеи ООН A/RES/74/247 от 27 декабря 2019 г. «Противодействие использованию информационно-коммуникационных технологий в преступных целях» и предварявшая ее резолюция Генеральной Ассамблеи ООН A/RES/73/187 от 17 декабря 2018 г.

в 27 Исследовательской комиссии по разработке международных стандартов информационной безопасности и нескольких подкомитетах, в том числе, по стандартам для искусственного интеллекта, Интернета вещей, 5G и робототехники. Задачу международной стандартизации ИКТ регион считает приоритетной.

В целях выполнения своего мандата МСЭ-Т ведет работу в регионе ЛАГ по ряду направлений, в том числе, по оказанию содействия слабо развитым странам. В частности, реализуются программы и проекты, одобренные в 2012 году на Саммите по проблемам связи в Дохе (Connect Arab Summit). Так, МСЭ выделил $450 млн на создание национальных групп реагирования CERT в 15 государствах-членах ЛАГ (оборудование и программное обеспечение, менеджмент, подготовка кадров). Это способствовало росту уровня готовности и национального потенциала для анализа вредоносного программного обеспечения, проведения технических экспертиз и расследований, повышения осведомленности.

В рамках Глобальной программы кибербезопасности МСЭ (GCA) при содействии Омана в декабре 2012 г. создан Арабский региональный центр кибербезопасности (ITU-ARCC). Он действует как платформа повышения осведомленности в регионе по вопросам информационной безопасности, для координации региональных инициатив в этой сфере, а также достижения целей GCA. Базируется ITU-ARCC и обслуживается национальной группой реагирования Омана (OCERT).

Арабский форум по управлению Интернетом (ArabIGF)

Форум по управлению Интернетом (IGF) создан во исполнение резолюции Всемирного саммита по информационному обществу в Тунисе. Впоследствии к нему добавились региональные форумы. В частности, арабский ArabIGF создан в 2012 г. на основании решения Экономической и социальной комиссии для Западной Азии ООН и Лиги арабских государств. Собирается ежегодно или раз в два года как этап подготовки региона к IGF.

Главными задачами форума являются выработка единой политики по приоритетам развития управления Интернетом для учета ее в глобальной повестке, содействие развитию надежной и безопасной инфраструктуры и передовых технологий, повышение человеческого потенциала. В 2017 г. выработана вторая редакция Арабской дорожной карты по управлению Интернетом, причем в ней вопросы кибербезопасности не только поднялись выше по списку, но и проходят красной нитью через все остальные задачи.

Приоритеты ЛАГ в IGF в порядке убывания важности:

1. Значительное улучшение инклюзивности — снижение различных барьеров по доступу к сети и повышение его удобства, в том числе через использование родного языка, развитие системы арабских доменных имен, преодоление дискриминации по любому признаку, в том числе гендерному.

2. Повышение доверия и безопасности киберсреды, в том числе через развитие правовых структур и систем на национальном и международном уровнях, сохранение целостности сети Интернет, приватности и права собственности пользователей; повышение транспарентности в использовании информации о поведении в сети пользователей и открытости политики использования данных.

3. Институциональное укрепление через участие в глобальном процессе выработки более сбалансированной, доступной, интернациональной и транспарентной схемы управления Интернетом (основные вопросы — прозрачность Организации по управлению адресами (IANA), системы корневых серверов и доменных имен).

4. Внедрение инноваций и передовых экосистем, открывающих новые возможности для экономического и социального развития, гарантия их безопасности (в том числе Интернета вещей и блокчейн).

5. Гуманитарное развитие, включая правозащитные вопросы, вовлечение молодежи и защита детей, повышение роли сети Интернет для решения социальных проблем и снятия барьеров между различными сегментами общества. Повышение потенциала и осведомленности в сфере кибербезопасности, развитие сотрудничества.

6. Критические структуры Интернета и его инфраструктура (система корневых серверов и файлы корневой зоны, доменные имена, адресация в сети, технические стандарты, а также инновационные конвергентные технологии, т.е. совокупность ИКТ, биотехнологий, нанотехнологий и различных когнитивных технологий).

7. Культурное и лингвистическое разнообразие — увеличение цифрового контента, отражающего арабскую культуру, другие культуры и локальные группы региона (появление ресурсов на арабском языке резко повысило использование социальных медиа).

Поднимаются и более конкретные проблемы, в частности в 2019 году на Пятом форуме ArabIGF обсуждались вопросы информационной безопасности, международных норм и право закона, вопросы конфликтов в киберпространстве и кризисное управление, дезинформация и шпионаж.

3. Форматы работы над региональной политикой кибербезопасности

Проблемы в выработке единой политики ЛАГ в развитии ИКТ и обеспечении безопасности их использования очевидны и носят объективный характер.

Ближний Восток и Северная Африка завязаны сложным узлом культурного единства и неразрешимых противоречий. Многие страны погрязли в политических конфликтах и даже войнах.

Государства региона существенно различаются по экономическому развитию. По данным Всемирного банка, опубликованным в 2020 г., ВВП Саудовской Аравии был в 20 раз выше, чем у Судана ($700 млрд против $34 млрд).

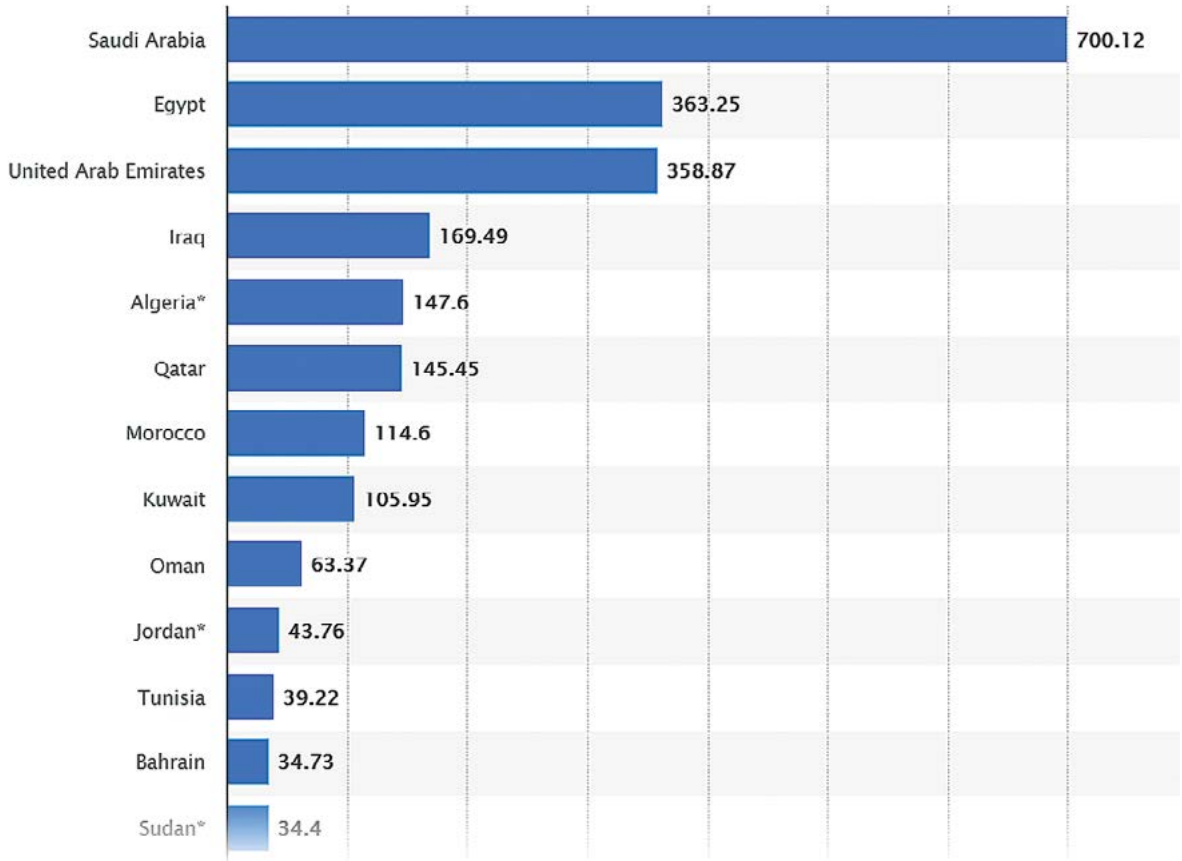


Схема 2. Уровень ВВП государств-членов ЛАГ.
Источник: Всемирный банк, 2020

Как следствие, уровень информатизации стран региона радикально отличается (см. Таблицу 1, стр. 30). Например, в Катаре в период с 2000 по 2021 год проникновение Интернета возросло в 100 раз, и сейчас страна является мировым лидером, оставив позади даже ОАЭ и Кувейт, где доступ в глобальную сеть имеет 100% населения. В противоположность этому Джибути по данному показателю находится в конце глобального рейтинга.

Следует отметить, что значительная доля региональных пользователей применяет для выхода в сеть смартфоны, но в государствах Персидского залива они есть у 75% населения, в Северной Африке — у 52%, а в остальных арабских странах всего у 38%. Проникновение мобильной связи в Мавритании, Судане и Йемене стабильно растет, но большинство людей по-прежнему не имеют доступа к Интернету. Соответственно, у некоторых государств-членов ЛАГ национальная политика в области информационной безопасности носит фрагментарный характер и пока не соответствует уникальным вызовам безопасности, характерным для региона.

Традиционно экономики стран-членов ЛАГ слабо интегрированы между собой, вектор экономических отношений направлен на глобальное сотрудничество. Из приведенных ниже диаграмм МСЭ следует следующее. Обмен трафиком напрямую между государствами-членами ЛАГ практически отсутствует (см. схему 3, которая имеет

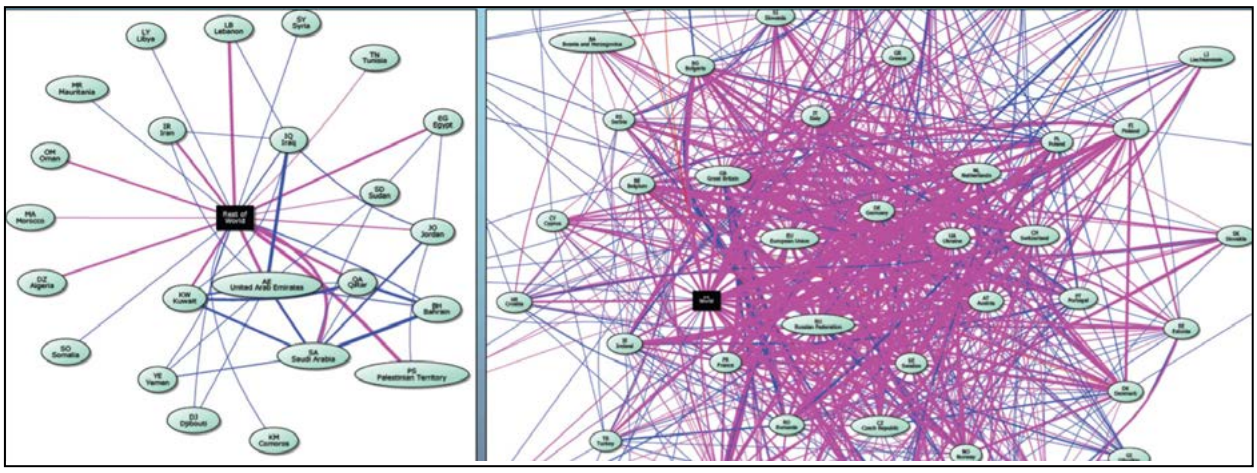


Схема 3. Схема 4.

Источник: Reality And Perspectives Of Internet Exchange Points In The Arab Region, 2019

структуру звезды с центром — внешними по отношению к объединению странами). Это свидетельствует о слабом развитии внутрирегиональных сетей связи, что является серьезным барьером к успеху цифровой экономики и электронной торговли в ЛАГ.

Схема 4 является наложением на Схему 3 трафика ЛАГ с другими государствами, что показывает глубину интеграции региона в глобальную экономику и информационный обмен.

В силу этих объективных причин страны региона имеют разные концепции национальной политики в области обеспечения информационной безопасности и участия в системе обеспечения МИБ. Существенное влияние на формирование этих концепций оказало исторически сложившееся сотрудничество в области кибербезопасности с западными партнерами (что отражается даже в терминологической базе). Вместе с тем последствия «арабской весны» заставили ЛАГ внимательно отнестись к сформированной Бразилией концепции «демократического» Интернета, но с большими оговорками по государственному контролю распространяемых в сети материалов. В частности, Египет, как и Россия, трактует понятие «информационная безопасность» широко и включает в него воздействие на сознание граждан. Следует отметить, что в регионе уголовное преследование за «ненадлежащее» использование Интернет одно из самых суровых.

Несмотря на разность подходов, а порою и расхождений по основополагающим вопросам, государства региона остро нуждаются в согласованной политике и гармонизации нормативных баз. Этой проблемой занимаются различные специализированные организации ЛАГ.

Их деятельность постепенно институализируется, обрастает различными форматами государственно-частного партнерства.

Схема 5. Система органов управления ЛАГ в сфере обеспечения информационной безопасности

Арабская организация по коммуникациям и информационным технологиям (AICT)

В 2021 г. по обобщенным итогам влияния пандемии COVID-19 на состояние безопасности киберпространства AICT опубликовала доклад «The Arab Vision For Cybersecurity: Reality–Challenges–Opportunities». Он содержит анализ состояния кибербезопасности в регионе и наиболее актуальных угроз, а также намечает возможные шаги по улучшению ситуации и снижению дисбаланса потенциалов государств-членов ЛАГ в сфере кибербезопасности. (см. Схему 6 и Таблицу 1 стр. 30).

По сути, указанный доклад является первым шагом к разработке единой стратегии региона в этой сфере с опорой на имеющийся мировой опыт. Кроме того, он обозначает рамки совместных действий и помощи отдельным государствам Лиги, чтобы выступать единым фронтом ради повышения благосостояния граждан и процветания всех арабских государств в цифровую эпоху.

Арабская конференция по безопасности (Arab Security Conference)

Эта площадка является на данный момент наиболее эффективным инструментом государственно-частного партнерства в рассматриваемой сфере, объединяя усилия государственного сектора, крупнейших региональных и глобальных

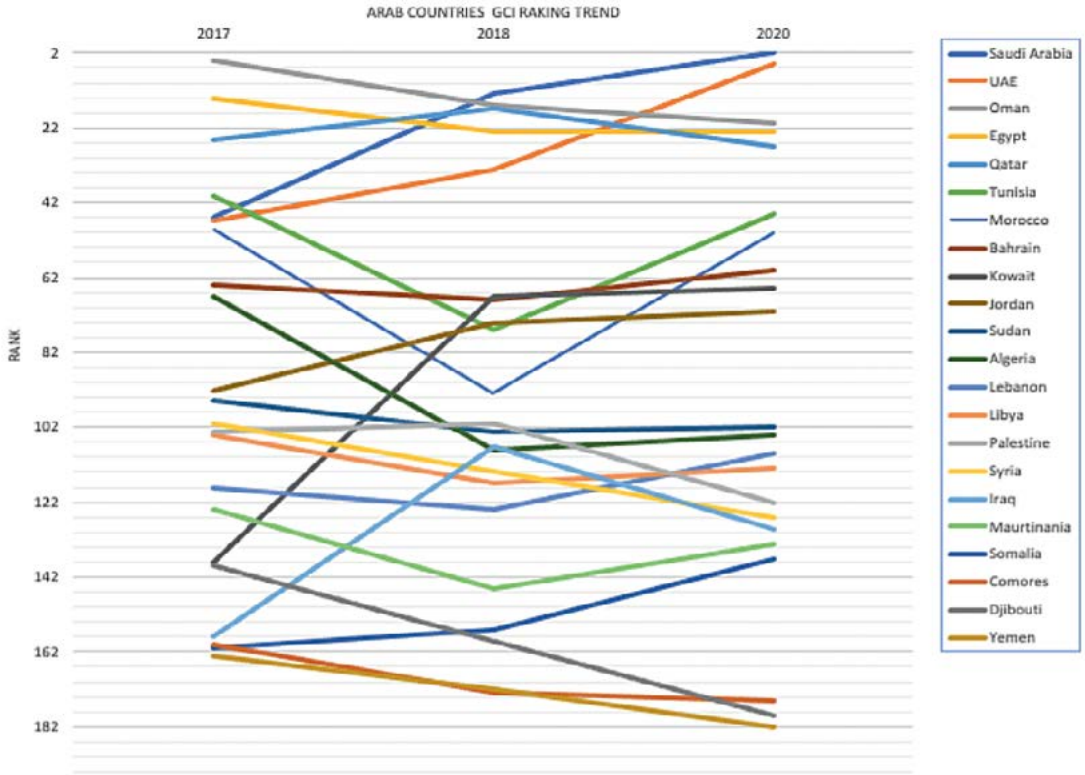


Схема 6. Динамика изменения позиции государств-членов ЛАГ в Глобальном рейтинге кибербезопасности МСЭ 2017–2020 гг.

Источник: Global Cybersecurity Index 2020, ITU

операторов и провайдеров ИКТ, компаний кибербезопасности, научного сообщества и НПО.

Конференция с 2017 г. проводится ежегодно в разных государствах Лиги. Организуется Арабским региональным центром кибербезопасности (ITU-ARCC), что, по сути, означает деятельное участие в этом МСЭ. Главной особенностью конференции является обсуждение, наряду с общей повесткой МСЭ, важных для региона проблем кибербезопасности, среди которых можно выделить социальный инжиниринг в контексте внутренних угроз, авиационную и спутниковую кибербезопасность, внедрение передовых ИКТ.

По примеру Сингапурской кибернедели эта конференция проводится в формате «недели повышения осведомленности по вопросам кибербезопасности» и включает широкий набор различных мероприятий. Наиболее значительные из них следующие:

- Арабский региональный саммит по кибербезопасности
- Конференция по кибербезопасности групп реагирования
- Финалы арабских премий по кибербезопасности и арабских соревнований по кибербезопасности *(Arab Security Cyber Wargames Championship и Regional Cyber Stars competition)*, которые традиционно используются

для рекрутинга талантливой молодежи в госсектор и ведущие компании кибербезопасности.

Глобальный форум по кибербезопасности (Global Cybersecurity Forum)

Форум является национальной инициативой Саудовской Аравии. Он собирает уникальное количество высокопоставленных участников со всего мира. В 2022 г. страна председательствовала в G20, поэтому указанному форуму придавалось очень большое значение и его темой было заявлено «Переосмысление глобального киберпорядка».

4. Нормативная база ЛАГ по кибербезопасности

На данный момент все нормативные документы ЛАГ в сфере информационной безопасности не имеют прямого действия:

- В 2010 году Лигой арабских государств принята Конвенция по борьбе с использованием информационных технологий в преступных целях. После получения ратификационных документов от 7 стран Конвенция вступила в силу 6 апреля 2014 г. Она носит рамочный характер и определяет общие принципы, на которых должны быть разработаны национальные законы в этой сфере. Большое внимание уделено укреплению сотрудничества между государствами для создания возможности защиты своих интересов, активов и населения от преступлений, совершаемых с использованием ИКТ. Как было отмечено ранее, Конвенция также создает правовые основы для противодействия использованию Интернета в террористических целях.
- В 2012 году разработан еще один рамочный документ, затрагивающий государства-члены ЛАГ — проект конвенции Африканского союза о создании юридических основ кибербезопасности в Африке. Эта Конвенция способствует обеспечению и поддержанию людских, финансовых и технических ресурсов, необходимых для содействия расследованию киберпреступлений.
- Конвенция Африканского союза о кибербезопасности и защите персональных 2014 года содержит в числе прочих положений призыв принимать национальные законы и/или вносить поправки в действующие национальные правовые акты с целью эффективной борьбы с киберпреступностью, унифицировать национальные законодательства, заключать договоры о взаимной правовой помощи, способствовать обмену информацией между государствами, содействовать региональному, межправительственному и международному сотрудничеству

и использовать имеющиеся средства для сотрудничества с другими государствами и даже с частным сектором.

5. Роль внешних факторов в формировании региональной повестки в области информационной безопасности и МИБ

В условиях роста полицентричности ведущие политические игроки ведут борьбу за сохранение стратегического влияния на этот важный для мировой экономики и глобальной безопасности регион.

США

Соединенные Штаты Америки, в том числе руками Евросоюза, НАТО и Израиля, скоординированно борются за сдерживание присутствия КНР на Ближнем Востоке и Африке как в части внедрения китайских ИКТ, так и финансирования НИОКР в сфере информационной безопасности. В последнее время тактика действий США в регионе изменилась. Американцы планомерно завышают киберпотенциал Ирана и угрозы государствам региона с его стороны. Под лозунгом «развития национального потенциала» по различной проблематике ЛАГ втягивается в подконтрольные США международные форумы и форматы сотрудничества.

Кроме того, США активно налаживают двустороннее сотрудничество на негосударственном уровне. В частности, в 2018 г. Саудовская федерация кибербезопасности и программирования (SFCSP) подписала меморандумы о взаимопонимании с Lockheed Martin, Raytheon Company, Northrop Grumman — основными корпорациями, которые обеспечивают информационную безопасность американского госсектора и сотрудничают с АНБ.

Выявлено несколько субсидированных США программ обучения и проведения исследований в университетах Ливана, Катара и Саудовской Аравии.

НАТО

Альянс в рамках своих программ глобальной безопасности стремится усилить свое влияние на Ближнем Востоке, в Северной Африке и за их пределами. Для НАТО наращивание оборонного потенциала на южном фланге позволит вести тесную совместную работу с региональными учреждениями безопасности, такими как Африканский союз и Лига арабских государств, а также с отдельными странами-партнерами.

Израиль включен в зону ответственности Центрального командования вооруженных сил США (CENTCOM), которое координирует оборонные операции США на Ближнем Востоке со своими партнерами и в качестве основных угроз отдает приоритет Ирану и террористическим группировкам.

Проект администрации Д. Трампа по созданию киберкомандования «арабского НАТО» (Middle East Strategic Alliance, MESA) пока отложен как по соображениям отсутствия единства мнений, так и из-за сохраняющейся в регионе настороженности к действиям США.

Израиль

В значительной степени Израиль давно является проводником реализации «мягкой силы» США в регионе Ближнего Востока и Северной Африки. Еще в 1981 году в рамках американской Ближневосточной программы регионального сотрудничества организовано взаимодействие египетских и израильских ученых, к которому в 1993 году примкнули Иордания, Ливан, Марокко, Тунис, Западный берег реки Иордан и Сектор Газа.

Сейчас это влияние усилено. В 2020 году при участии США заключены т.н. «Соглашения Авраама» о мире и восстановлении дипломатических отношений между Израилем и ОАЭ, а также между Израилем и Бахрейном. При посредничестве США были достигнуты договоренности по урегулированию конфликта в Западной Сахаре, что также способствовало развитию сближения Израиля с Марокко и Суданом.

Эти события серьезно изменили роль Израиля в региональной кибербезопасности, сделав его гарантом защиты от киберугроз со стороны Ирана. В частности, в июле 2021 г. заключено соглашение между военными ведомствами Марокко и Израиля о сотрудничестве в области киберобороны и радиоэлектронной борьбы, оперативном сотрудничестве, совместном проведении необходимых НИОКР, обмене информацией и знаниями. Однако против сближения с Израилем предостерегают Алжир и Кувейт.

Следует отметить, что предоставление Израилем инструментов обеспечения информационной безопасности государствам-членам Совета сотрудничества арабских государств Персидского залива (ССАГПЗ) началось давно. Например, 2007 году ОАЭ привлекли израильскую компанию 4D Security Solutions, базирующуюся в США, для повышения киберзащиты важных энергетических объектов и создания системы наблюдения в Абу-Даби с использованием искусственного интеллекта. Также налажен обмен разведывательной информацией о действиях ливанских хакерских группировок, связанных с Хизбаллой.

Израиль, обладая высоким научным потенциалом, является разработчиком средств проникновения в информационные системы и контроля поведения пользователей. По некоторым данным, Марокко, Бахрейн, Саудовская Аравия и ОАЭ применяли для слежки за диссидентами шпионское программное обеспечение Pegasus, разработанное израильской компанией NSO Group.

Не утихают слухи и об американо-израильском происхождении вируса Stuxnet, примененного в отношении ядерных объектов Ирана.

Препятствиями успешности в ЛАГ кибертандема США-Израиль являются значительное присутствие Китая в финансировании израильских НИОКР и высокотехнологичных стартапов, а также собственные геополитические интересы Израиля.

КНР

Китай осуществляет обширную программу технологической и финансовой экспансии в Африке и регионе MENA (страны Магриба и Ближнего Востока). Кроме того, с участием большинства этих стран он реализует проект «Цифровой шелковый путь» по строительству континентальной магистрали связи Юго-Восточной Азии с Европой, являющейся альтернативой подводной системе кабелей через Персидский залив. Эти действия наносят серьезный удар по интересам США, поэтому борьба за влияние на ЛАГ может иметь последствия для этих государств-членов Лиги, что требует от последних тонкого политического маневра. Саудовская Аравия и ОАЭ тяготеют к Вашингтону, но не хотят портить отношения с основным импортером своей нефти, поведение других стран имеет свои нюансы.

В марте 2021 г. ЛАГ и КНР объявили о заключении соглашения о сотрудничестве в разработке глобальных стандартов безопасности данных (China-LAS Cooperation Initiative on Data Security). Это означает, что регион поддерживает китайскую Глобальную инициативу по безопасности данных, а не американскую Инициативу чистой сети, которая делит все каналы связи на «чистые» (фактически подконтрольные США) и «нечистые».

Китайская компания Huawei тесно сотрудничает с Арабским союзом Интернета и телекоммуникаций (ARISPA), активно используя политику транспарентности своих технологий (в 2021 году компанией инвестировано более $1 млн в НИОКР по кибербезопасности, по всему миру создано 7 центров транспарентности). Развитие сетей 5G будет не только повышать качество связи внутри региона, но и давать государствам Персидского залива ежегодный доход в $273 млрд (по текущим оценкам).

Евросоюз

Европейская политика в Средиземноморье (ENP) основана на принятой в 2016 году Глобальной стратегии политики в области иностранных дел и безопасности (EUGS). Она включает значительный по объему раздел по кибербезопасности, направленный на создание «общей» культуры безопасности за счет повышения возможностей ближайших соседей к защите от киберугроз.

С Алжиром, Иорданией, Ливаном, Марокко и Тунисом Евросоюз реализует целый пакет сотрудничества по борьбе с киберпреступностью «CyberSouth» и противодействию терроризму CEPOL CT 2, в рамках которого планируется усовершенствовать правовые рамки и институциональные возможности сбора электронных доказательств.

Десять государств-членов ЛАГ (Алжир, Египет, Ирак, Иордания, Ливан, Ливия, Марокко, Палестина, Сирия, Тунис) участвовали в программе ЕС по наращиванию потенциала правоохранительных органов, разведки и полиции для борьбы с терроризмом «CT MENA Counter-Terrorism in the Middle East and North Africa» (2017–2020). В 2018 году завершилась программа ЕС и Иордании по выявлению скрытого экстремизма, но запущены две новые: по управлению кризисами и наращиванию потенциала в сфере кибербезопасности.

Таким образом, несмотря на то, что большинство государств-членов ЛАГ не присоединились к Будапештской конвенции по киберпреступности (за исключением Марокко и находящегося в процессе адаптации национальной нормативной базы к требованиям Конвенции Туниса), форматы взаимодействия в этой сфере основаны на европейских подходах. Для укрепления этого взаимодействия выдвигаются идеи разработки единой ЕС-Средиземноморской киберстратегии.

Следует также отметить, что некоторые виды помощи в наращивании потенциала в сфере кибербезопасности ЛАГ осуществляются в рамках программ технической помощи или финансируются за счет глобальных инициатив ЕС.

6. Перспективы сотрудничества Российской Федерации с ЛАГ в сфере развития ИКТ и обеспечения МИБ

Важной спецификой ЛАГ в решении вопросов информационной безопасности является ориентация на глобальное, а не на региональное сотрудничество.

Значительное финансовое и технологическое присутствие в регионе ведущих в этой сфере игроков, а также наличие сложного баланса интересов сокращают возможности вхождения новых участников.

Вместе с тем существенные различия в национальных концепциях обеспечения кибербезопасности государств-членов ЛАГ, а также различный уровень их потребностей создают благоприятные условия для сотрудничества по отдельным взаимовыгодным направлениям.

При этом следует учитывать специфику ментальности арабского региона, выбирать лишенные политической окраски, прагматичные сферы сотрудничества, соблюдать деликатность в предложении содействия. Выгода сотрудничества должна быть оценена партнерами самостоятельно. Действия США через «мягкую силу» дают пример долгосрочной стратегии, позволяю-

щей через неформальные контакты на экспертном уровне прокладывать путь к политическим решениям.

Исходя из этого, а также учитывая уровень зрелости национальных политик в сфере цифровизации и киберзащиты, в Таблице 3 (стр. 32) приведена интегральная экспертная оценка перспектив сотрудничества с государствами-членами ЛАГ.

По результатам проведенного анализа можно рекомендовать следующие направления сотрудничества с ЛАГ, которые имеют высокие перспективы развития:

- поддержка проводимых ЛАГ международных конференций, привлечение государств-членов Лиги к российским мероприятиям
- развитие мультистейкхолдерной модели управления Интернетом за счет поиска решений на уровне общественных и частных организаций
- сотрудничество по вопросам развития электронного правительства
- научные проекты по различным вопросам кибербезопасности
- экспертное сотрудничество по выработке международных стандартов для передовых технологий
- продвижение российских продуктов кибербезопасности посредством увеличения их транспарентности, в том числе за счет совместной разработки технологий
- обмен опытом по правовому регулированию информационной безопасности и противодействия киберпреступности.

Рисунок 1. Архитектура взаимодействия Лиги арабских государств с региональными организациями

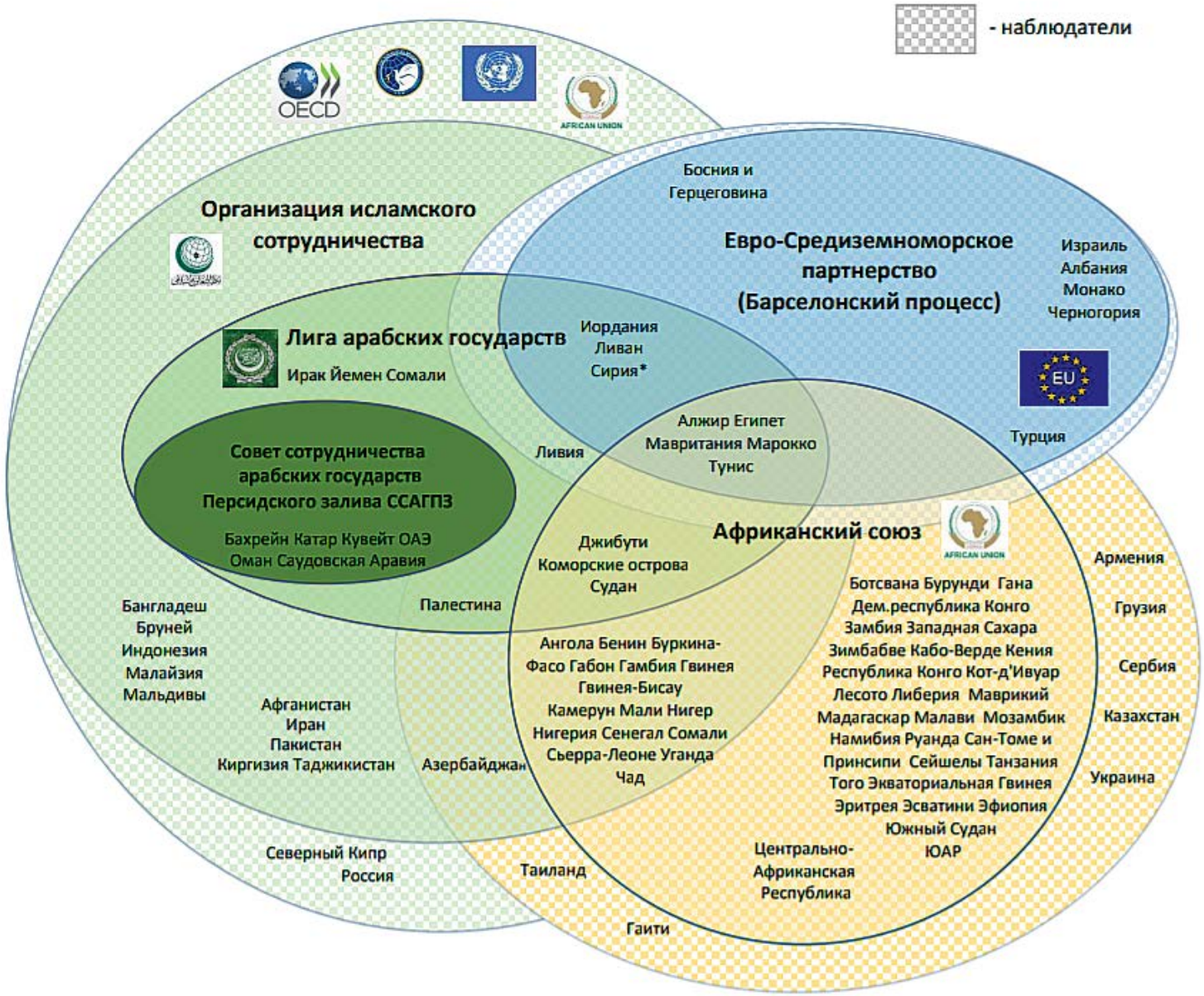
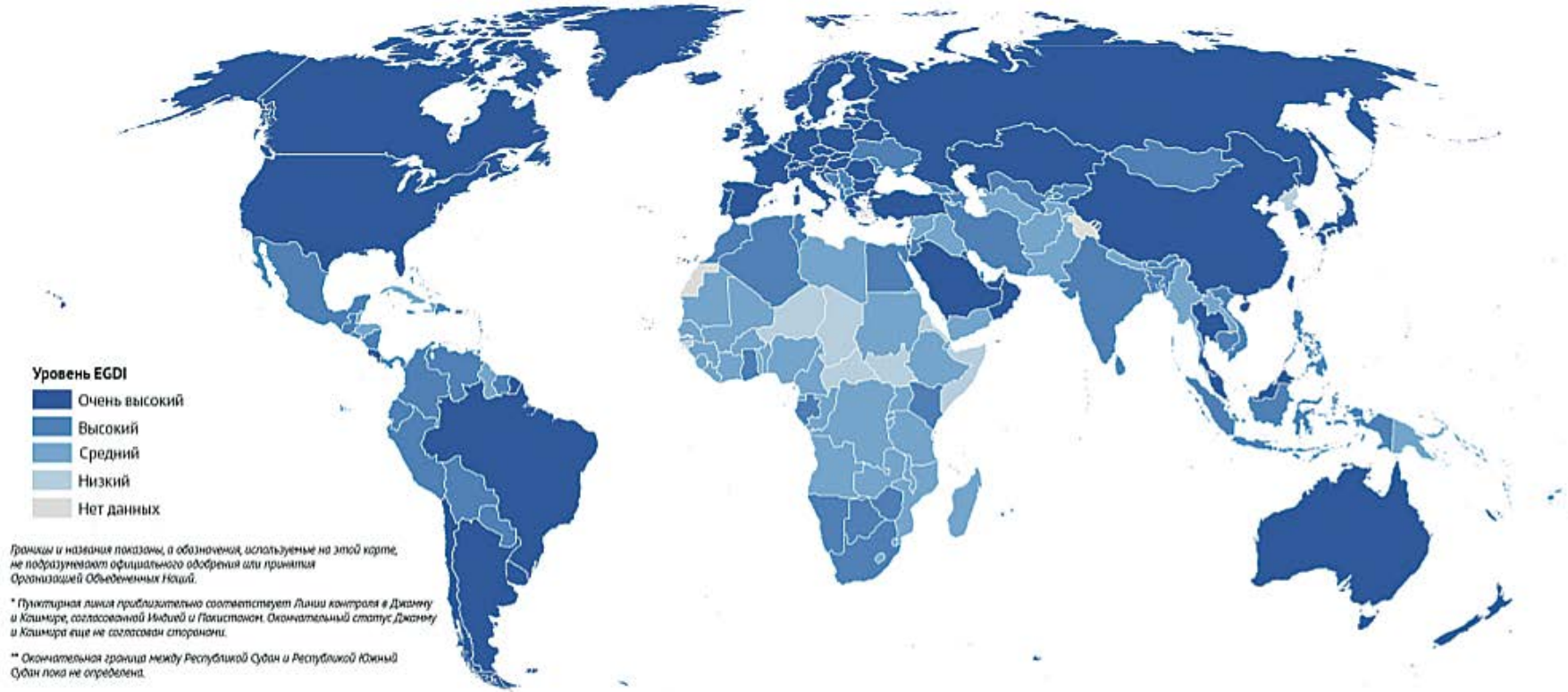


Рисунок 2. Карта развития электронных правительств в мире



По состоянию на 2020 год на карте отображены страны с очень высоким, высоким, средним и низким уровнем EGDI — Индекса развития электронного правительства, разработанного Управлением ООН по экономическим и социальным вопросам, который учитывает объем и качество онлайн обслуживания, индекс развития ИКТ инфраструктуры и человеческий капитал.

Источник: Исследование ООН: Электронное правительство 2020 Цифровое правительство в десятилетии действий по достижению устойчивого развития С дополнением по реагированию на COVID-19, 2020

Таблица 1. Лига арабских государств: основные показатели эффективности государственной политики в сфере ИКТ и информационной безопасности

		МСЭ 2021	МСЭ Глобальный индекс кибербезопасности GCI 2021			NCSI Бангалорский институт кибербезопасности					UN DESA	UNIDIR	
	Государства-члены Лиги арабских государств	Уровень проникновения Интернет (%)	Индекс развития гос. политики	Рейтинг в ЛАГ	Рейтинг в мире	Уровень цифрового развития	Индекс готовности к киберугрозам и реагированию	Стратегия развития ИКТ/ цифровизации	Стратегия кибер. безопасности	Программа развития искусств. инт-та	Уровень развития эл. правительства	Национальная группа реагирования	Национальное законодательство в сфере кибер преступности
1.	Алжир	57	33.95	**12**	104	42.81	33.77	2015	—	2021	выс	DZ-CERT 1985	2009 , 2016
2.	Бахрейн	97.8	77.86	**8**	60	66.04	25.97	2009	2019	2019	выс	CERT.bh 2014	2002, 2014, 2017
3.	Джибути	54.8	1.73	**21**	179	*	*	*	—	—	ср	—	—
4.	Египет	52.5	95.48	**4**	23	46.93	57.14	2012	2018	2020	выс	EG-Cert 2009	2018
5.	Иордания	84.7	70.96	**10**	71	54.07	28.57	2020	2012, 2018	2020	выс	JO-CERT 2017	2007, 2015 2019
6.	Ирак	91.8	20.71	**17**	129	*	*	*	*	*	*	Iraq Cyber Events Response Team 2018	1969, 2014
7.	Йемен	25.9	0	**22**	182	18.00	7.79	2001	*	*	ср	YemenCERT	2022*
8.	Катар	104.3	94.5	**5**	27	64.96	55.84	2019	2014	2019	оч.в	QCERT 2008	2014
9.	Коморы	21.8	3.72	**20**	175	*	*	*	2019*	*	ср	—	2020
10.	Кувейт	98.3	75.05	**9**	65	—	—	—	2017	—	выс/оч.в	NCSC 2018	2016
11.	Ливан	81.3	30.44	**13**	109	—	19.48	—	2019*	—	ср/в	ECERT	2018
12.	Ливия	84.2	28.78	**14**	113	41.10	10.39	*	*	*	ср	Libya-Cert 2013	—
13.	Мавритания	72.2	18.94	**18**	133	11.30	11.69	*	*	*	ср	CERT-MU 2008	2003, 2016
14.	Марокко	68.5	82.41	**7**	50	46.88	23.38	2013	2011	2021*	выс	MACERT 2013	2003
15.	ОАЭ	103.3	98.06	**2**	5	68.01	40.26		2019	2017	выс	aeCERT 2008	2006, 2012, 2018
16.	Оман	76.8	96.04	**3**	21	60.34	33.77	2003 2020	2017	2020	выс/оч.в	OCERT 2010	2008, 2011
17.	Палестина	64.8	25.18	**15**	122	*	*	*	*	*	*	*	2018
18.	Сауд. Аравия	90.1	99.54	**1**	2	63.46	83.12	2016	2013, 2020	2017	выс	CERT-SA 2006	2007
19.	Сирия	46.5	22.14	**16**	126	33.40	15.58	2009	2014	—	ср/в	ISC 2011	2012
20.	Сомали	12.8	17.25	**19**	137	*	*	2014	—	—	низ	—	—
21.	Судан	29.2	35.03	**11**	102	25.50	11.69	*	—	—	ср	SudanCERT 2017	2007
22.	Тунис	68.4	86.23	**6**	45	46.26	46.75	*	2018	2020	выс	tunCERT 2017	1999

* - недостаточно данных

Таблица 2. Позиции государств-членов ЛАГ при голосовании по наиболее значимым резолюциям ГА ООН по МИБ

		ГПЭ 2015 итог	РГОС созыв 2019- 2021	РГОС итог 2019-2021 и созыв 2021-2025	ГПЭ созыв 2019-2021	ГПЭ итог 2019-2021	Подготовка к Спецком. по конвенции	Созыв Спецком. по конвенции
		A/RES/70/237 от 23.12.2015 (без голосования)	A/RES/73/27 от 5.12.2018	A/RES/75/240 от 31.12.2020	A/RES/73/266 от 22.12.2018	Доклад A/76/135 (принят членами ГПЭ)	A/RES/73/187 от 17.12.2018	A/RES/74/247 от 27.12.2019
1.	Алжир	соавтор	соавтор	соавтор	воздержались		соавтор	соавтор
2.	Бахрейн		За	За	За		За	воздержались
3.	Джибути	соавтор	За	За	За		воздержались	воздержались
4.	Египет	соавтор	За	За	против		соавтор	соавтор
5.	Иордания		За	За	За		За	За
6.	Ирак		За	За	За		За	За
7.	Йемен	соавтор	За	За	За		За	За
8.	Катар		За	За	За		За	За
9.	Коморы		За	соавтор, не голос	против		не голосовали	За
10.	Кувейт		За	За	За		За	За
11.	Ливан		За	За	За		За	За
12.	Ливия		За	воздержались	За		соавтор	соавтор
13.	Мавритания		За	За	За		За	За
14.	Марокко	соавтор	За	За	За		За	воздержались
15.	ОАЭ	соавтор	За	За	За		За	За
16.	Оман	соавтор	За	За	За		За	За
17.	Палестина		За	За	За		За	За
18.	С. Аравия		За	За	За		За	воздержались
19.	Сирия	соавтор	соавтор	соавтор	против		соавтор	соавтор
20.	Сомали		не голосовали	не голосовали	За		За	За
21.	Судан	соавтор	За	За	За		соавтор	соавтор
22.	Тунис		За	За	За		не голосовали	воздержались

Таблица 3. Экспертная оценка перспектив развития сотрудничества

нет | низкая | средняя | высокая

		В сфере МИБ и управления Интернетом			Научно-техническое сотрудничество					Повышение потенциала/ обмен опытом	
		На уровне гос. ведомств	На уровне частного бизнеса	На уровне ГЧП и НПО	Развитие ИКТ инфраструктур (не донорство)	Приобретение российских технологий ИБ	Группы реагирования CERT (сверх типового)	Кооперация в сфере межд. стандартов	Совместные научные проекты	в сфере развития электронного правительства	в сфере правового регулирования кибербезопасности
1.	Алжир										
2.	Бахрейн										
3.	Джибути										
4.	Египет										
5.	Иордания										
6.	Ирак										
7.	Йемен										
8.	Катар										
9.	Коморы										
10.	Кувейт										
11.	Ливан										
12.	Ливия										
13.	Мавритания										
14.	Марокко										
15.	ОАЭ										
16.	Оман										
17.	Палестина										
18.	Сауд. Аравия										
19.	Сирия										
20.	Сомали										
21.	Судан										
22.	Тунис										

III. Анализ нормативной базы Лиги арабских государств и Африканского союза в сфере обеспечения информационной безопасности

1. Арабская Конвенция о борьбе с преступлениями в сфере информационных технологий 2010 года

Арабская Конвенция (далее — Конвенция) о борьбе с преступлениями в сфере информационных технологий была принята в 2010 году в целях укрепления сотрудничества между арабскими странами «в борьбе с преступлениями в области информационных технологий, угрожающими их безопасности, интересам и безопасности их сообществ» и позволила сторонам «принять общую уголовную политику, направленную на защиту арабского общества от преступлений в области информационных технологий». Конвенция была подписана арабскими странами, в том числе всеми шестью государствами-членами ССАГПЗ. Однако, говоря о предотвращении киберпреступности в рамках ССАГПЗ, аналитики придерживаются мнения, что сотрудничество стран Персидского залива в борьбе с киберпреступностью в большей или меньшей степени основывается на двусторонних отношениях и неофициальных каналах, таких как сотрудничество между полицией или ведомствами. Хотя эти механизмы полезны, но они недостаточны для эффективного режима, поскольку накладывают ограничения на следственные действия, не имеют общего подхода и должны действовать в рамках нескольких правоохранительных сетей. Неофициальные механизмы обычно служат предшественниками официальных запросов о заключении Договоров о взаимной правовой помощи (MLAT), которые представляют собой «соглашения между правительствами, способствующие обмену информацией, относящейся к расследованию, проводимому по крайней мере в одной из этих стран».

Хотя Арабскую конвенцию критиковали за ее расплывчатые формулировки, неадекватность определений, ее положения фактически почти такие же, как положения Будапештской конвенции, особенно в отношении процедурных полномочий и международного сотрудничества, двух основных элементов, отсутствующих в большинстве законов о киберпреступности стран Персидского залива.

Очевидно, что ССАГПЗ необходимо изучить дальнейшие варианты укрепления регионального и международного сотрудничества. При этом он должен смотреть на то, что выполнимо и практично. Одним из возможных направлений действий может быть изучение каналов активизации Конвенции, которая обеспечивает полезную платформу для сотрудничества в судебной области и, по крайней мере, была подписана всеми странами Персидского залива. Дру-

гой возможностью для государств-членов ССАГПЗ было бы получение статуса наблюдателя в рамках Будапештской конвенции, чтобы узнать о Конвенции и определить, могут ли они присоединиться к ней и каким образом. В качестве альтернативы государства Персидского залива могли бы полагаться на Конвенцию Организации Объединенных Наций против транснациональной организованной преступности (UNTOC), которую они ратифицировали, поскольку она предоставляет широкие возможности для международного сотрудничества в сфере борьбы с киберпреступностью, что в некоторых случаях может создать платформу для взаимодействия.

2. Конвенция Африканского союза «О кибербезопасности и защите персональных данных» от 27 июня 2014 г.

Изучение нормативной базы Африканского союза в области информационной безопасности (кибербезопасности) в контексте анализа соответствующих правовых актов Лиги арабских государств представляется важным с учетом одновременного членства в Африканском союзе десяти государств из состава ЛАГ (Алжир, Джибути, Египет, Коморские острова, Ливия, Мавритания, Марокко, Сомали, Судан и Тунис).

Африканский союз — международная межправительственная организация, объединяющая 55 государств Африки. Основана 9 июля 2002 г. Правопреемник Организации африканского единства (ОАЕ).

Важнейшие решения в рамках организации принимаются на Ассамблее Африканского союза — собрании глав государств и правительств государств-членов организации, которое проводится раз в полгода.

Секретариат Африканского союза расположен в столице Эфиопии Аддис-Абебе.

Вопросам содействия кибербезопасности и борьбе с киберпреступностью посвящена глава III (статьи 24–31) Конвенции Африканского союза «О кибербезопасности и защите персональных данных» от 27 июня 2014 г. (далее — Конвенция).

Часть 1 (статьи 24–28) определяет меры по обеспечению кибербезопасности, которые должны быть приняты на национальном уровне.

Часть 2 (статьи 29–31) раскрывает уголовные положения.

В Конвенции к киберпреступлениям отнесены:

- атаки на компьютерные системы (шесть составов преступлений);
- атаки на компьютерную информацию (шесть составов преступлений);
- преступления, связанные с содержанием компьютерной информации (восемь составов преступлений, связанных главным образом с детской порнографией и экстремизмом);

- преступления, связанные с электронными сообщениями;
- имущественные преступления, совершаемые с использованием информационно-коммуникационных технологий (четыре состава преступлений).

Конвенция налагает на государства-члены обязательства по принятию правовых, политических и нормативных мер для содействия управлению кибербезопасностью и борьбы с киберпреступностью.

В Конвенции обосновывается необходимость создания регионального механизма мониторинга в рамках Африканского союза для улучшения региональной гармонизации механизмов управления кибербезопасностью и применения Конвенции в качестве основы для содействия региональной кибербезопасности.

2.1 Определение кибербезопасности и киберстабильности

В Конвенции понятие «кибербезопасность» определяется как «совокупность инструментов, политик, руководящих принципов, подходов к управлению рисками, действий, обучения, передовой практики, гарантий и технологий, которые могут быть использованы для защиты киберсреды и организаций, а также активов пользователей».

Указывается, что меры по управлению кибербезопасностью включают технические, организационные, политические и юридические аспекты.

Делается акцент на том, что технические аспекты управления кибербезопасностью касаются разработки и внедрения технических мер защиты компьютерных систем и сетевой инфраструктуры, в то время как организационные аспекты касаются развития институционального потенциала для содействия кибербезопасности. Например, создание правоохранительных организаций, а также Групп реагирования на компьютерные чрезвычайные ситуации (CERT) для предоставления услуг критически важным объектам, таких, как предотвращение и раннее предупреждение, обнаружение и управление инцидентами кибербезопасности.

Политические и правовые аспекты управления кибербезопасностью касаются политических и правовых мер, направленных на содействие кибербезопасности.

Правовые меры обычно рассматриваются как наиболее важный аспект борьбы с киберпреступностью. Такие меры включают принятие законов, запрещающих действия, нарушающие безопасность, целостность или доступность компьютерных данных и систем или сетей, а также атаки на критически важную информационную инфраструктуру.

Также Конвенция включает в себя правовые меры по содействию трансграничному сотрудничеству в области кибербезопасности, включая предотвращение, расследование и судебное преследование запрещенных действий.

Предусмотренная концепция киберстабильности определена как «геостратегическое условие, при котором пользователи киберпространства получают максимально возможные выгоды для политической, гражданской, социальной и экономической жизни, предотвращая и управляя поведением, которое может подорвать эти выгоды на национальном, региональном и международном уровнях».

Это создает основу для определения того, когда стабильность является целью, а также, что потенциально является актуальной, полезной и стратегической информацией о деятельности в киберпространстве, а что нет.

По сути, концепция киберстабильности направлена на содействие осуществлению государственных обязанностей по решению проблем безопасности информационного общества. Это, в частности, требует принятия государствами в пределах своей юрисдикции соответствующих правовых, политических и нормативных мер для защиты киберпользователей и информационной инфраструктуры, а также обеспечения того, чтобы кибердеятельность, осуществляемая в пределах их юрисдикции, не причиняла вреда другим лицам или инфраструктуре в другой юрисдикции.

Также концепция киберстабильности требует, чтобы государства приняли меры по управлению кибербезопасностью, включая уголовные законы (такие, как законы и правила о киберпреступности), с целью удержания лиц, находящихся под их юрисдикцией, от участия в злонамеренной деятельности, которая причинит вред другим лицам или инфраструктуре в другой юрисдикции.

По-видимому, необходимость содействия киберстабильности возникает в связи с увеличением взаимосвязанности национальных информационно-коммуникационных сетей в разных странах, что привело к эпохе сетевой взаимозависимости, когда безопасность сети каждой страны также зависит от действий государственных и негосударственных субъектов по всему миру.

В целом концепция киберстабильности предусматривает, чтобы государства сохраняли ответственность за управление кибердеятельностью на своей территории, и, таким образом, в ней закреплены элементы международных принципов трансграничного ущерба и ответственности государств.

2.2 Обязательства государств-членов по осуществлению мер, способствующих кибербезопасности

Конвенция устанавливает следующие обязательства государств-членов по осуществлению мер, способствующих кибербезопасности:

- создание национальной системы кибербезопасности, включая поощрение культуры кибербезопасности;
- создание национальных структур управления кибербезопасностью;

- защита критически важной информационной инфраструктуры (КИИ);
- установление преступлений, связанных с киберпреступностью, и процессуальные меры;
- содействие международному сотрудничеству и гармонизации законодательства.

2.3 Обязательства по созданию национальной системы кибербезопасности

Конвенция требует, чтобы государства-члены содействовали киберстабильности путем создания соответствующих механизмов управления кибербезопасностью.

В связи с этим государства-члены должны создать национальную систему кибербезопасности, которая включает национальную политику и национальную стратегию в этой сфере.

Национальная политика государства-члена в области кибербезопасности должна признавать важность национальной КИИ и определять связанные с ней риски с использованием подхода «all-hazards» (*все-опасности*), а также как должны быть достигнуты цели такой политики.

Подход «all-hazards» к защите КИИ предполагает защиту такой инфраструктуры от всех форм угроз, независимо от того, исходят ли они от преднамеренных нападений, несчастных случаев или стихийных бедствий.

Кроме того, обязательство разработать национальную политику в области кибербезопасности требует от государств-членов изложить, как их национальная политика в области кибербезопасности будет способствовать достижению целей защиты национальных КИИ от выявленных рисков.

Что касается разработки национальной стратегии кибербезопасности, статья 24:2 Конвенции требует, чтобы государства-члены принимали стратегии, которые они считают «надлежащими и адекватными» при осуществлении своей национальной политики в области кибербезопасности, особенно при осуществлении таких инициатив, как правовая реформа и развитие, наращивание потенциала, международное сотрудничество в рамках государственно-частного партнерства и повышение осведомленности о кибербезопасности.

В связи с этим в Конвенции признается суверенное право каждого государства-члена принимать любую стратегию, которую оно сочтет подходящей или целесообразной для эффективной реализации своей национальной политики в области кибербезопасности.

Обязательства в соответствии со статьей 24:2 Конвенции также требуют, чтобы национальная стратегия кибербезопасности государства-члена:

- определяла организационные структуры для управления кибербезопасностью;
- устанавливала цели и сроки для успешной реализации национальной политики в области кибербезопасности;
- создавала важнейшую основу для эффективного управления инцидентами в области кибербезопасности и международного сотрудничества в таких вопросах.

Примечательно, что требование Конвенции о том, чтобы государства-члены устанавливали политику и стратегии кибербезопасности, в значительной степени схоже со статьей 7 Директивы Европейского союза о сетевой и информационной безопасности (NIS Directive, 2016), которая также требует, чтобы государства-члены приняли «национальную стратегию безопасности сетевых и информационных систем, определяющую стратегические цели и соответствующие политические и нормативные меры с целью достижения и поддержания высокого уровня безопасности сетевых и информационных систем [...]».

2.4 Обязательства по созданию национальных структур управления кибербезопасностью

Статья 25:2 Конвенции налагает на государства-члены обязательства по созданию соответствующих структур или учреждений, а также по регулированию полномочий, необходимых для управления кибербезопасностью.

Статья 27:1(a) требует, чтобы государства-члены «приняли необходимые меры для создания соответствующего институционального механизма, обеспечивающего управление кибербезопасностью».

В значительной степени положения указанных статей Конвенции аналогичны статье 8(1) вышеуказанной Директивы ЕС, которая требует, чтобы государства-члены «назначили один или несколько национальных компетентных органов по безопасности сетевых и информационных систем».

В соответствии с Конвенцией обязательства по созданию национальных структур управления кибербезопасностью требуют создания соответствующих национальных учреждений, отвечающих за борьбу с киберпреступлениями и реагирование на инциденты в области кибербезопасности, а также за содействие международному сотрудничеству в управлении такими инцидентами.

Таким образом, в контексте этих обязательств подразумевается, что каждое государство-член должно создать такие учреждения, как национальное агентство по кибербезопасности и национальная CERT.

Конвенция также требует, чтобы были созданы национальные структуры управления кибербезопасностью, которые могли бы реагировать на вызовы

и проблемы, затрагивающие все аспекты кибербезопасности на национальном уровне.

В целях обеспечения эффективного функционирования национальных структур кибербезопасности Конвенция требует, чтобы государства-члены приняли необходимые меры для установления подотчетности по вопросам кибербезопасности на всех уровнях государственного управления путем определения ролей и обязанностей учреждений в однозначных и точных выражениях, а также выражения четкой публичной и прозрачной приверженности продвижению кибербезопасности, включая поощрение участия частного сектора в правительственных инициативах по продвижению кибербезопасности.

2.5 Обязательства по защите КИИ

Конвенция устанавливает обязательства государств-членов по защите КИИ. В этом отношении статья 25:4 Конвенции требует, чтобы государства-члены приняли необходимые законодательные и нормативные меры для определения тех секторов, которые «чувствительны» к их национальной безопасности и экономическому благополучию, а также классифицировали системы ИКТ, предназначенные для функционирования в этих секторах, как элементы КИИ.

Хотя Конвенция не дает в прямой постановке определение понятию КИИ, она, тем не менее, классифицирует его в увязке с термином «Критическая кибер/ИКТ инфраструктура», который в соответствии со статьей 1 Конвенции определяется как «киберинфраструктура, которая необходима для жизненно важных служб обеспечения общественной безопасности, экономической стабильности, национальной безопасности, международной стабильности и для устойчивости и восстановления критически важного киберпространства».

Обязательства по защите КИИ в соответствии со статьей 25:4 Конвенции требуют, чтобы государства-члены устанавливали строгие санкции за киберпреступления и другие преступные действия, которые влияют на системы ИКТ в важнейших секторах, а также принимали меры по повышению безопасности и управлению такими системами.

Статья 30:1(d) Конвенции устанавливает обязательство по защите КИИ, которое требует, чтобы государства-члены «приняли необходимые меры уголовного законодательства для ограничения доступа к защищенным системам, которые классифицируются как критическая инфраструктура национальной обороны из-за содержащихся в них важных данных о национальной безопасности».

Конвенция прямо не классифицирует сектора, которые следует рассматривать как «чувствительные» применительно к национальной безопасности и экономическому благополучию государств-членов.

Вероятно, отсутствие такой классификации связано с различиями в подходах государств-членов к оценкам секторов, которые могли бы быть обозначены как «чувствительные».

Однако общая тенденция в установлении такой классификации заключается в том, что длительное нарушение функционирования сектора или инфраструктуры может повлиять на благосостояние государства, вызвав серьезные экономические потрясения или проблемы национальной безопасности. В этом случае такой сектор или инфраструктура обычно рассматриваются как «чувствительные» применительно к национальной безопасности и экономическому благополучию государства и, следовательно, классифицируются как «критический сектор» или «критическая инфраструктура».

В целом большинство секторов, которые классифицируются как критические, в значительной степени зависят от элементов систем ИКТ, таких как компьютерные технологии и цифровые сети, для эффективного функционирования. Следовательно, эти элементы систем ИКТ в важнейших секторах классифицируются как КИИ. Поэтому концепция КИИ обычно используется для обозначения основных элементов ИКТ, включая взаимосвязанные и взаимозависимые информационные сетевые системы, которые жизненно важны для функционирования важнейших секторов и основных услуг в современных обществах.

Суть установления обязательств по защите КИИ проистекает из растущего проникновения ИКТ в Африку, что привело к их растущей интеграции в секторах, которые можно классифицировать как критические. Эта растущая интеграция ИКТ в важнейших секторах также рассматривается как средство содействия экономическому развитию Африки и региональной интеграции.

Однако, хотя африканские государства не достигли высокого уровня цифровизации, сопоставимого с развитыми странами, ее рост в Африке усилил зависимость важнейших секторов от элементов ИКТ, а также взаимосвязанных и взаимозависимых информационных сетевых систем в той мере, в какой разрушение такой инфраструктуры в результате несчастных случаев или злонамеренных действий может привести к нарушению экономической и социальной деятельности, а также государственных услуг и, тем самым, вызвать проблемы национальной безопасности.

Таким образом, необходимо отметить, что африканские государства также уязвимы для угроз кибербезопасности, которые затрагивают элементы важнейших секторов, которые полагаются на информационную инфраструктуру, обычно классифицируемую как КИИ.

Указанные факторы подчеркивает причины, по которой статья 25:4 Конвенции направлена на усиление защиты КИИ в Африке путем наложения обяза-

тельств на государства-члены Африканского союза по принятию соответствующих правовых и политических мер.

2.6 Обязательства по установлению преступлений, связанных с киберпреступностью, и процессуальные меры

Статья 25:1 Конвенции налагает на государства-члены обязательства по криминализации основных преступных деяний, которые влияют на конфиденциальность, целостность, доступность и долговечность систем ИКТ и данных, обрабатываемых такими системами.

Это подразумевает, что государства-члены обязаны устанавливать преступления, которые криминализируют такие действия, как несанкционированный доступ к компьютерной системе, несанкционированное вмешательство в компьютерную систему или данные, а также несанкционированный перехват данных, обрабатываемых компьютерной системой.

Кроме того, статья 25:1 Конвенции требует от государств-членов криминализации основных преступных деяний, затрагивающих сетевую инфраструктуру ИКТ. Это влечет за собой установление состава преступлений, предусматривающих уголовную ответственность за нападения на КИИ.

Конвенция также требует от государств-членов четко криминализировать преступления, связанные с киберпреступностью, включая:

- атаки на компьютерные системы;
- несанкционированный доступ к компьютерным системам;
- действия, препятствующие функционированию компьютера;
- несанкционированное изменение компьютерных данных;
- несанкционированный перехват компьютерных данных;
- подделка компьютерных данных;
- компьютерное мошенничество;
- преступления, связанные с детской порнографией;
- подготовительные преступления, связанные с неправомерным использованием компьютерных устройств, такие как незаконное производство, продажа, импорт, владение или предоставление компьютерного оборудования, программы или любого устройства или данных, которые «разработаны или специально адаптированы» для целей совершения любого киберпреступления.

В некоторой степени требование Конвенции о том, чтобы государства-члены криминализировали вышеуказанные преступления в области киберпреступности, схоже с некоторыми обязательствами в соответствии с Директивой ЕС о нападениях на информационные системы (2013). Она, в частности, требует от государств-членов криминализировать незаконный доступ к информационным

системам, незаконное вмешательство в информационные системы, незаконное вмешательство в данные и незаконный перехват данных.

Статья 25:1 Конвенции также налагает на государства-члены обязательства по созданию эффективных процедурных механизмов для судебного преследования за киберпреступления.

Такие процедурные механизмы в основном предназначены для расширения правовых возможностей правоохранительных органов по расследованию и судебному преследованию преступлений, связанных с киберпреступностью, и они обычно включают меры по облегчению поиска, изъятия или сохранения цифровых доказательств или перехвата электронных сообщений.

При разработке правовых мер по борьбе с киберпреступлениями государства-члены также должны учитывать выбор формулировок, используемых в передовой международной практике. Это подразумевает, что государства-члены должны рассмотреть вопрос о выборе формулировок, используемых в международных документах и типовых законах о киберпреступности, таких как Конвенция Совета Европы о киберпреступности и Инструментарий МСЭ для законодательства о киберпреступности.

Очевидно, что это обязательство направлено на то, чтобы побудить государства-члены разработать основные и процедурные правовые меры по борьбе с киберпреступностью на технологически нейтральном языке в целях содействия международной гармонизации национальных законов о киберпреступности и процедурных мер.

Кроме того, статья 25:3 Конвенции требует, чтобы государства-члены обеспечивали, чтобы разработка и осуществление правовых мер по управлению кибербезопасностью не нарушали конституционные права граждан, такие как право на свободу выражения мнений, право на неприкосновенность частной жизни, право на справедливое судебное разбирательство и другие основные права, которые защищены национальным или международным правом, в том числе в соответствии с Африканской Хартией прав человека и народов.

Это требование в некоторой степени схоже с подходом, Конвенции Совета Европы о киберпреступности, которая требует от государств-членов обеспечить, чтобы их процессуальные инструменты для расследования и судебного преследования киберпреступлений не нарушали основные права человека.

2.7 Обязательства по содействию международному сотрудничеству и гармонизации законодательства

Конвенция устанавливает рамки для содействия международному сотрудничеству в области кибербезопасности и борьбы с киберпреступностью в рамках Африканского союза.

В связи с этим государства-члены должны «поощрять создание учреждений, которые обмениваются информацией о киберугрозах и оценке уязвимости, таких как Группы реагирования на компьютерные чрезвычайные ситуации (CERT) или Группы реагирования на инциденты компьютерной безопасности (CSIRTs)».

Статья 28:4 Конвенции также требует, чтобы государства-члены «использовали существующие каналы международного сотрудничества с целью реагирования на киберугрозы и улучшения кибербезопасности и стимулирования диалога между заинтересованными сторонами».

Такие каналы могут основываться на международных, межправительственных или региональных соглашениях или партнерских отношениях между частным и государственным секторами.

В целях содействия эффективной гармонизации правовых норм и международного сотрудничества между государствами-членами статья 28:1 Конвенции устанавливает обязательства государств-членов «обеспечивать, чтобы законодательные меры и/или нормативные акты, принятые для борьбы с киберпреступностью, расширяли возможности региональной гармонизации [...] и соблюдали принцип двойной уголовной ответственности».

Статья 28:2 Конвенции также предусматривает, что государства-члены, у которых нет соглашений о взаимной правовой помощи в борьбе с киберпреступностью, «обязуются поощрять подписание соглашений о взаимной правовой помощи в соответствии с принципом двойной уголовной ответственности, одновременно содействуя обмену информацией, а также эффективному обмену данными между организациями [государств-членов] на двусторонней и взаимной основе».

Это означает, что государства-члены, у которых отсутствуют соглашения о взаимной правовой помощи в борьбе с киберпреступностью, обязаны их заключать.

3. Выводы

Недостаточная эффективность в сфере управления кибербезопасностью стала решающим фактором, который повлиял на рост в африканских государствах негативных тенденций в области киберпреступности.

Принятие Конвенции подтвердило понимание серьезности указанных проблем, стало свидетельством нацеленности Африканского союза на их решение путем принятия мер содействия обеспечению кибербезопасности, по крайней мере с региональной точки зрения.

Достижение заявленных в Конвенции целей, направленных на содействие обеспечению региональной киберстабильности, в большей степени зависит от выполнения государствами-членами обязательств, вытекающих из Конвенции, а также от способности Африканского союза координировать и контролировать эту деятельность.

IV. Развитие политики в сфере информационной безопасности и информационных технологий

1. АЛЖИР

Официальное название: Алжирская Народная Демократическая Республика
Столица: Алжир
Официальные языки: арабский и берберский

Территория: 2 381 740 км² (10-я в мире). Пустыня Сахара занимает 80% территории страны и состоит из отдельных песчаных (Большой Западный Эрг, Большой Восточный Эрг, Эрг-Игиди, Эрг-Шеш) и каменистых (плато Танезруфт, Тингерт, Тадемаит, Эль-Эглаб) пустынь. На юго-востоке алжирской Сахары приподнято нагорье Ахаггар, где находится высшая точка Алжира — гора Тахат (2908 м). Со всех сторон нагорье окружено ступенчатыми плато Тассилин-Адджер, Тассилин-Ахаггар и горами Муйдир. Север алжирской Сахары лежит на 26 м ниже уровня моря. Здесь расположено соленое озеро Шотт-Мельгир.

Население: 46 653 000 чел. (по оценкам на 2021 год), что является 33-м показателем в мире.

Государственное устройство: Согласно конституции Алжир — президентско-парламентская республика. Глава государства — президент, избираемый населением на 5-летний срок.

Парламент Алжира — законодательный (представительный) орган. Совет нации — 144 места, треть назначается президентом, две трети избираются непрямыми выборами на 6-летний срок. Национальная народная ассамблея — нижняя палата Парламента Алжира — состоит из 407 мест, избираемых населением на 5-летний срок по пропорциональной избирательной системе в 59 многомандатных избирательных округах, соответствующих 58 провинциям (вилайетам) страны, плюс один округ, представляющий диаспору за рубежом. Каждому округу выделяется количество мест в зависимости от его населения: одно место на сегмент в 120 тыс. жителей, плюс одно место для любого оставшегося сегмента в 60 тыс. жителей, минимум три места на избирательный округ. Партийные списки открытые, с преимущественным голосованием и избирательным барьером в 5% от поданных голосов. После подсчета голосов распределение мест производится в соответствии с методом, известным как «самый сильный остаток».

Экономика: Показатели Валового внутреннего продукта (ВВП) (Паритет покупательной способности) за 2019 год:

- Итого: $509,307 млрд (42-й показатель в мире)
- На душу населения: $11 729 (107-й показатель в мире)

Показатели ВВП (Номинал) за 2019 год:

- Итого: $169,267 млрд. (53-й показатель в мире)
- На душу населения: $3898 (113-й показатель в мире)

Дипломатические отношения с Россией (СССР): установлены 23 марта 1962 г.

1. Уровень развития системы обеспечения информационной безопасности и информационно-коммуникационной инфраструктуры (включая индекс развития ИКТ по оценкам МСЭ и ООН)

Исходя из перечисленных ниже статистических данных, уровень развития системы информационной безопасности Алжира может быть оценен как низкий:

МСЭ 2021, индекс кибербезопасности: 33,95 (из 100)
МСЭ 2021, позиция в рейтинге среди государств ЛАГ: 12
МСЭ 2021, позиция в глобальном рейтинге: 104
МСЭ, уровень проникновения Интернет: 57%
NCSI, уровень цифрового развития: 42,81
NCSI, индекс готовности к киберугрозам и реагированию на них: 33,77

2. Основные документы стратегического планирования в области обеспечения информационной безопасности

Указ Президента Алжира (январь 2020 г.) «О создании национального механизма безопасности информационных систем, разработке национальной стратегии безопасности информационных систем и координации ее реализации».

Предусматривает создание:

- Совета, ответственного за разработку национальной стратегии безопасности информационных систем;
- Агентства, ответственного за координации реализации национальной стратегии безопасности информационных систем.

Создание данных структур позволит установить контроль и определить стандарты защиты информационных систем.

Реализация национальной стратегии нацелена:

- ✓ на повышение готовности национальной информационной инфраструктуры к защите от киберрисков и киберугроз;
- ✓ на подготовку молодых специалистов высокого уровня в области кибербезопасности;
- ✓ на повышение культуры кибербезопасности.

Национальная стратегия исследований и инноваций в области искусственного интеллекта (ИИ) на 2020–2030 годы.

Национальная стратегия разработана в январе 2021 г. под эгидой Министерства высшего образования и научных исследований.

Цели Стратегии:

- ✓ повышение уровня Алжира в области ИИ посредством обучения и исследований;
- ✓ наращивание потенциала ИИ как инструмента развития, позволяющего социально-экономическим секторам устранять препятствия, сдерживающие переход к цифровым технологиям;
- ✓ повышение уровня исследований в стратегических технологических областях.

3. Основные угрозы информационной безопасности и общие подходы к противодействию этим угрозам, в том числе основные направления обеспечения информационной безопасности, включая используемые ключевые институты и инструменты защиты

Внешние угрозы

В качестве основных внешних угроз рассматриваются киберугрозы, исходящие от Франции, Израиля и Марокко и реализуемые ими с использованием, в том числе, территорий третьих стран.

Хактивизм:

- ✓ использование киберпространства и, в частности, социальных сетей и форумов для анонимного обсуждения политических вопросов, продвижения идей или поддержки прав;
- ✓ перенос протеста и гражданского неповиновения в киберпространство, попытка изменить политику, используя кибероружие;
- ✓ возможность выражать себя во всем мире без необходимости объединять тысячи людей в одном месте для общения.

Воздействие, как правило, осуществляется в несколько этапов:

- ✓ первый этап — использование социальных сетей для вербовки хактивистов, передача им инструкций и инструментов атаки или кибероружия;
- ✓ второй этап — распознавание и раскрытие уязвимостей веб-сайта;
- ✓ третий этап — DDoS-атака и кража данных.

Противодействие данному виду угроз планируется принятием превентивных мер для защиты сетей от такого рода деятельности, в том числе за счет:

- ✓ устранения существующих уязвимостей на веб-сайтах;
- ✓ выбора активного подхода, отслеживающего деятельность хактивистов в специализированных социальных сетях и блогах во время кризисов или важных событий в стране.

Кибершпионаж

Оценивался в 2022 году как самая большая угроза, имеющая целью:

- ✓ наступательную деятельность в области кибербезопасности;
- ✓ тайный сбор из информационных сетей информации в области обороны и безопасности, экономики, внешней политики;
- ✓ получение преимущества над страной, доминирование над ней или использование ее во время кризиса для лоббирования.

Отмечается угроза развития возможностей кибершпионажа для их использования как на международной, так и на национальной арене, поскольку этот вид деятельности обеспечивает высокую доходность при относительно низких, если не нулевых, затратах и рисках.

У работающих в Алжире иностранных компаний Juniper и Fortinet были выявлены бэкдоры (дефекты алгоритма, которые намеренно встраиваются в него разработчиком и позволяют получить несанкционированный доступ к данным или удаленное управление операционной системой и компьютером в целом) в своих брандмауэрах (сетевые экраны для контроля и фильтрации входящего/исходящего трафика), которые должны были защищать сети от внешних кибервторжений.

Программы-шпионы

В качестве таких программ рассматриваются программное обеспечение:

израильской компании NSO, в том числе Pegasus, которое устанавливается на мобильный телефон, чтобы дистанционно управлять камерой, микрофоном и собирать все доступные на них данные за считанные секунды;

британской компании Circles Technologies, которое может отслеживать мобильный телефон на национальном или глобальном уровне (роуминг), подключаясь к инфраструктуре оператора, а не напрямую к целевому телефону.

Внутренние угрозы

Согласно отчету компании «Лаборатория Касперского» за 2020 год Алжир занял второе место по количеству оборудования, зараженного вредоносным программным обеспечением.

Чрезмерное заражение национального киберпространства сопряжено с тремя высокими рисками:

- ✓ во-первых, содействие атакам на национальные сети;
- ✓ во-вторых, использование хакерами этой архитектуры для организации атак на ненациональные сети и возложение ответственности за них на Алжир;
- ✓ в-третьих, возможность поставить под угрозу национальные проекты по цифровизации, предназначенные для развития страны.

Риск указанных угроз возрастает в связи с распространением в Алжире нетрадиционных средств покупки и оплаты, таких как электронная торговля и электронные платежи, что особенно проявляется в условиях зараженного киберпространства и отсутствия необходимых средств и систем безопасности.

В 2022 году отмечался рост использования алжирскими и иностранными киберпреступниками нового вектора атак банков и онлайн-платежных пунктов.

DDoS-атаки или отказ в обслуживании

В условиях высокой зависимости алжирских организаций от Интернета, как средства работы и предоставления услуг, возрастает ответственность подразделений ИТ-безопасности не только за защиту инфраструктуры, но и за устранение рисков, вызванных ростом числа атак типа отказ в обслуживании (DDoS), которые сегодня считаются одной из наиболее серьезных угроз доступности информационных ресурсов.

В 2020 году наиболее подвержены атакам были компании беспроводной связи, которые зафиксировали увеличение количества DDoS-атак на 64%.

Программы-вымогатели

В качестве основной угрозы рассматриваются программы-вымогатели, прекращающие доступ к файлам или загрузку компьютера, а затем принуждающие жертв к выплате выкупа за возвращение системы в нормальное состояние.

Наиболее опасными считаются программа-вымогатель Locker (запрещает пользователям доступ к основным функциям их компьютеров) и программа-вымогатель Crypto (шифрует данные — на ее долю приходится 75% атак).

В Алжире в 2020 году количество атак-вымогателей выросло на 200% по сравнению с 2019 годом, при этом, по оценкам экспертов, данные атаки носят целенаправленный характер.

4. Участие в международном сотрудничестве в области формирования системы обеспечения международной информационной безопасности в рамках ООН и позиция при голосовании по наиболее важным резолюциям ГА ООН

Алжир активно поддерживает российские инициативы в области международной информационной безопасности, всегда выступая в их поддержку.

В 2018–2020 годах являлся соавтором российских проектов резолюций Генеральной Ассамблеи ООН:

A/RES/73/27 от 5 декабря 2018 г. (принятие правил, норм и принципов ответственного поведения, а также создание Рабочей группы ООН открытого состава);

A/RES/73/187 от 17 декабря 2018 г. (включение в повестку дня ООН обсуждения вопроса о противодействии использованию ИКТ в преступных целях);

A/RES/74/247 от 27 декабря 2019 г. (создание специального межправительственного комитета экспертов открытого состава для разработки всеобъемлющей международной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях);

A/RES/75/240 от 31 декабря 2020 г. (создание новой Рабочей группы ООН открытого состава по вопросам безопасности в сфере использования ИКТ и самих ИКТ 2021–2025).

При голосовании за принятие американского проекта резолюции Генеральной Ассамблеи ООН A/RES/73/266 от 22 декабря 2018 г. (о создании Группы правительственных экспертов ООН на 2019–2021 годы) Алжир воздержался.

5. Участие в международном сотрудничестве с другими международными организациями в области формирования системы обеспечения информационной безопасности на региональном уровне

Алжир взаимодействует на глобальном и региональном уровнях по вопросам обеспечения кибербезопасности в рамках следующих международных организаций, членом которых он является:

ООН;

ITU (МСЭ);

Движение неприсоединения;

Африканский союз;

ЛАГ;

Интерпол;

ISO (Международная организация по стандартизации).

Также Алжир имеет соглашение об ассоциации с ЕС и является партнером для сотрудничества с ОБСЕ.

6. Содержание и оценка предложений и инициатив в области формирования системы обеспечения международной информационной безопасности

Представитель Алжира Фаузия Мебарки является председателем созданного в ООН по инициативе России специального межправительственного комитета экспертов открытого состава для разработки всеобъемлющей международной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях.

Алжир:

не стал соавтором инициативы Франции и Египта — Программа действий ООН по продвижению ответственного поведения государств в киберпространстве (2020 год);

не присоединился к инициативе Франции — Парижский призыв к доверию и безопасности в киберпространстве (2018 год).

2. БАХРЕЙН

Официальное название: Королевство Бахрейн

Столица: Манама

Официальный язык: арабский

Территория: 701 км² (176-я в мире). Бахрейн расположен на 33-х островах архипелага Бахрейн. Самый крупный остров — Бахрейн протягивается с севера на юг — 50 км, с запада на восток — 15 км. Этот остров сложен известняками, а остальные — кораллового происхождения. В центре острова находится плато высотой 30–35 м, самой высокой точкой является гора Эд-Духан (134 м).

Население: 1 451 200 чел. (по оценкам на 2017 год), что является 153-м показателем в мире.

Государственное устройство: Бахрейн — дуалистическая монархия. Во главе государства стоит король (до 2002 года — эмир). Правительство возглавляет премьер-министр. Кабинет состоит из 23 министров. Парламент — двухпалатный. Нижняя палата — Палата депутатов избирается на всенародном голосовании, верхняя — Консультативный совет (Меджлис аш-Шура) назначается королем. В обеих палатах заседает по 40 человек.

Экономика: Показатели ВВП (Паритет покупательной способности) за 2019 год:

- Итого: $76,994 млрд (101-й показатель в мире)
- На душу населения: $51 892 (19-й показатель в мире)

Показатели ВВП (Номинал) за 2019 год:

- Итого: $38,574 млрд (94-й показатель в мире)
- На душу населения: $25 998 (37-й показатель в мире)

Дипломатические отношения с Россией (СССР): установлены 29 сентября 1990 г.

1. Уровень развития системы обеспечения информационной безопасности и информационно-коммуникационной инфраструктуры

Королевство Бахрейн является одним из самых информатизированных государств в мире, уровень проникновения сети Интернет в стране достиг 99%. Страна вошла в десятку лидеров по развертыванию высокоскоростных сетей подвижной связи 5G, в начале 2021 г. эта технология была внедрена на всей территории страны[1]. Хорошо развиты наземные сети широкополосного доступа, надежно интегрированные в глобальную сеть связи через несколько систем оптоволоконных подводных кабелей. По данным ООН, в арабском регионе Бахрейн является лидером по индексу развития ИКТ и индексу телекоммуникационной инфраструктуры. Совокупность перечисленных факторов позволяет Королевству претендовать на статус регионального центра предоставления передовых цифровых технологий.

В связи с этим государство уделяет повышенное внимание вопросам обеспечения кибербезопасности. Результаты проведенного анализа статистических данных и отчетов компаний информационной безопасности показывают, что защищенность национального информационного пространства высокая. По данным МСЭ, за 2021 год интегральный индекс кибербезопасности Бахрейна, рассчитанный с учетом развития правовой системы обеспечения информационной безопасности, применяемых технических и организационных мер, реализации программ наращивания потенциала и участия в международном сотрудничестве, составил 77,86 (из 100). Это ставит Бахрейн на 60-ю позицию в мире и на 8-ю среди государств-членов ЛАГ по обеспечению информационной безопасности.

2. Основные документы стратегического планирования в области обеспечения информационной безопасности

2.1. Стратегия экономического развития «Видение-2030»

Высоких результатов в области обеспечения информационной безопасности и развития ИКТ удалось достичь за счет принятия в 2008 г. долгосрочной стратегии социально-экономического развития Bahrain Economic Vision-2030. Она определила курс на диверсификацию экономики за счет цифровизации и развития комплексного подхода к государственной политике в области ИКТ и информационной безопасности. Достижение целей Видение-2030 обеспечивается реализацией среднесрочных и краткосрочных документов стратегического планирования.

1 Общая площадь всех островов, составляющих территорию Королевства Бахрейн, меньше площади Москвы в пределах МКАД, а население, даже с учетом большого количества экспатов, составляет менее 1,5 млн. чел.

2.2. Стратегии и планы развития отрасли ИКТ

Первый Национальный план в области развития электросвязи[2] был принят в 2003 году. Его основной целью было улучшение доступа к услугам ИКТ для активизации экономического и социального развития.

За десять лет (2009–2019 годы) путем либерализации национального рынка телекоммуникаций в ИКТ-сектор удалось привлечь более $2 млрд инвестиций. Не последнюю роль в этом сыграло выгодное географическое положение страны, а также прямая заинтересованность США. Бахрейн, начиная с 2002 года, является основным союзником НАТО вне блока[3] и предоставляет свою территорию для размещения американских военных баз[4]. Рядом со столичным городом Манама находится штаб-квартира Пятого флота ВМС США, где расположен один из четырех центров управления кибербезопасностью Глобальной информационной сети МО США. Не удивительно, что к точке обмена международным трафиком в Манаме подключено пять мощных подводных оптоволоконных кабелей, соединяющих Бахрейн с Европой, Юго-Восточной Азией и Африкой[5].

В настоящее время стратегия цифрового развития Бахрейна сфокусирована на следующих направлениях: расширение использования электронных сервисов; развитие государственно-частного партнерства в продвижении ИКТ-услуг; повышение цифровой грамотности населения и государственных служащих; достижение более высокого уровня знаний, навыков и сотрудничества; рост эффективности государственного управления; предложение качественных услуг электронного правительства и расширение их внедрения; развитие инноваций и предпринимательства.

В 2021 году за счет цифровой трансформации национальной экономики ИКТ-отрасль дала 3% ВВП. Значительный вклад дает использование возможностей технологии 5G[6] для развития финтеха, электронного правительства, электронной торговли, дистанционного образования, Интернета вещей и робототехники.

В январе 2022 г. обнародована Стратегия сектора телекоммуникаций, ИКТ и цифровой экономики на 2022–2026 годы, которая будет способствовать дости-

---

2 В настоящее время реализуется Пятый план в области развития электросвязи.

3 Это позволяет Бахрейну участвовать в совместных исследованиях и разработках, получать приоритетную поставку избыточных оборонных изделий и совместное обучение, финансируемое на взаимной основе.

4 На территории Королевства Бахрейн военных объектов США, из которых наиболее значимые: авиабаза Иса ВВС США, военно-морская база Naval Support Activity и база снабжения аль-Мухаррак, военная база аль-Джуфайр, база Пятого флота ВМС США и командного центра Сил специального назначения.

5 В Бахрейне «приземляются» 5 подводных кабелей (FOG, FALCON, GBICS, Tata TGN-Gulf, 2Africa), еще несколько находятся в стадии проектирования.

6 В стране действуют три конкурирующих оператора подвижной связи 5G, выбор поставщиков технологий правительством не ограничивается. Государственный оператор Batelco и телекоммуникационная группа Zain Bahrain сотрудничают со шведской Ericsson. VIVA Bahrain, дочерняя компания государственной телекоммуникационной компании STC, сотрудничает с Huawei.

жению целей экономического развития «Видение-2030». Среди основных направлений деятельности указаны:

- улучшение позиции Королевства Бахрейн в индексе развития электронного правительства, оцениваемого ООН;
- создание цифровой инфраструктуры мирового уровня путем разработки стандартов кибербезопасности, привлечения крупных технологических компаний и превращения страны в региональный центр цифровых инноваций;
- цифровая трансформация всех сфер деятельности, расширение использования в интересах экономики, управления и развития потенциала передовых технологий (искусственного интеллекта, Больших данных, блокчейн и Интернета вещей).

В результате реализации Стратегии планируется повысить инновационный потенциал (в ИКТ-секторе увеличить количество начинающих компаний на 20%), расширить функции электронного правительства (автоматизировать еще 200 государственных услуг), развить национальный человеческий капитал (увеличить занятость в ИКТ-секторе на 35% и подготовить не менее 20 тыс. граждан Бахрейна для работы в области кибербезопасности[7]). Важно отметить, что в отличие от других государств Персидского залива, по состоянию на 2020 год, Королевство не испытывало существенной зависимости от притока высококвалифицированных экспатов и обеспечивало ИКТ-отрасль на 71% национальными кадрами.

В 2017 году по решению Высшего комитета по информационно-коммуникационным технологиям, возглавляемого заместителем премьер-министра, начата реализация общенациональной политики «Сначала облако», следуя которой правительство и государственные учреждения обязаны рассматривать внедрение технологий облачных вычислений как неотъемлемую часть своих ИТ-планов и процессов.

В соответствии с указанной политикой на единых стандартах взаимодействия и безопасности в облачной инфраструктуре будут объединены государственные сети передачи данных, национальные Дата-центры и центры государственных услуг для получения доступа граждан, бизнеса, предприятий критической инфраструктуры и государственных учреждений.

Облачными технологиями будут эффективно пользоваться и коммерческие компании с применением различных моделей: бизнес-процессы как услуга (BPaaS), программное обеспечение, как услуга (SaaS), платформа как услуга (PaaS), инфраструктура как услуга (IaaS), что позволит существенно снизить затраты предприятий на оборудование, разработку и эксплуатацию[8].

---

7 Национальный фонд труда Tamkeen совместно с американским SANS Institute осуществляют подготовку 1,2 тыс. бахрейнцев в сфере программирования, кибербезопасности и работы с передовыми ИКТ, а также планируют создать для них в течение десяти лет 1 тыс. рабочих мест.

8 Поставщики ИКТ в Бахрейн в основном американские: Arista Networks, Broadcom, Cisco Systems, Dell, Hewlett Packard Enterprise, IBM, NetApp, Oracle; в незначительной доле китайские — Huawei, Lenovo.

Внедрение облачной концепции инициировало резкий рост предложений по строительству в Бахрейне передовых Дата-центров. Ожидается, что рынок инвестиций в их развитие будет ежегодно увеличиваться на 10–17% и к 2027 году составит $ 363 млн. Основными инвесторами на данный момент являются Batelco (Bahrain Telecommunications Company) и Zain Bahrain.

Уже действует 6 высокопроизводительных Дата-центров. Два из них принадлежат американской компании Amazon[9], которая привлечена в качестве официального поставщика облачной инфраструктуры для государственного сектора. По одному центру у бахрейнских компаний stc Bahrain, Zain Bahrain, Nuetel Communications, цифровой платформы Global Zone. В 2021 году объявлено о вхождении на этот рынок китайской компании Tencent Cloud для создания в регионе MENA первой общедоступной облачной инфраструктуры компании, а также эмиратской компании ATDXT LLC для строительства центра обработки данных в интересах Федерации цифровой экономики Лиги арабских государств (AFDE).

Существенным недостатком внедряемого тотального перехода в «облако» является полная зависимость страны от надежности и безопасности ИКТ сторонних производителей.

2.3. Стратегия электронного правительства eGovernment

Первые шаги по развитию услуг электронного правительства осуществлялись в рамках плана развития ИКТ-отрасли. В 2012 году была принята первая тематическая стратегия eGovernment, которая установила стратегические цели дальнейшего развития с учетом интересов и задач конкретных целевых групп: граждан и временно пребывающих на территории государства, бизнеса, государственных учреждений. Среди целей Стратегии указаны:

- развитие цифровых приложений, готовности ИКТ сектора и партнерств;
- повышение цифровой грамотности и навыков сотрудников государственного сектора;
- улучшение защиты данных и частной жизни граждан;
- повышение эффективности работы правительства;
- управление качеством предоставляемых услуг;
- ускорение внедрения инноваций и предпринимательства.

В результате выполнения задач стратегии 568 государственных услуг предоставляются в цифровом виде, из них 439 доступны через национальный портал, 19 — через киоски самообслуживания и 11 — с приложений на смартфонах. В течение 2021 года осуществлено создание полностью облачных государственных услуг для четырех ведомств (Национальное бюро по доходам, Национальный центр коммуникаций, Управление городского планирования и развития, Управ-

9 В 2019 году компания Amazon открыла в Бахрейне свой региональный офис.

ление по устойчивой энергетике); перенос 70% операций и систем 72 государственных организаций; полная миграция в облако 32 государственных и частных организаций. Это уже позволило сократить операционные расходы на 60–80% и повысить техническую готовность инфраструктуры.

Для обеспечения информационной безопасности государственных данных, размещенных в Дата-центрах, разработана политика обеспечения безопасности, которая предписывает ведомствам-собственникам информации провести ее классификацию в соответствии с Законом о государственной тайне и Руководящими принципами классификации государственных данных. Ведомства в сотрудничестве с уполномоченным на контроль выполнения указанной политики Комитетом по управлению ИКТ (ICTGC) должны разработать модель угроз и требования к контролю безопасности[10] всех категорий данных, выполнение которых должна обеспечить подрядная коммерческая организация (собственник Дата-центра). Таким образом, ответственность за обеспечение информационной безопасности распределяется между уполномоченным государством ведомством, собственником данных и подрядчиком.

2.4. Национальная Стратегия кибербезопасности (2017)

Первая Национальная стратегия кибербезопасности принята Бахрейном в 2017 году. Ее основной целью стала защита национальных интересов путем снижения киберугроз и создания безопасного национального информационного пространства. Среди целей были обозначены следующие:

- защита национальной критически важной инфраструктуры;
- выработка целостного подхода к реагированию на инциденты компьютерной безопасности в государственном и частном секторах;
- создание соответствующей международным стандартам законодательной и нормативной базы обеспечения информационной безопасности и борьбы с киберпреступностью;
- развитие экосистемы кибербезопасности, повышение осведомленности и культуры информационной безопасности;
- укрепление доверия граждан к онлайновым общественным системам, расширение услуг электронного правительства;
- международное сотрудничество по противодействию угрозам и наращиванию потенциала в информационном пространстве.

Для координации выполнения стратегии был создан Национальный комитет по кибербезопасности.

10 Меры контроля могут включать: физическую и объектовую безопасность, управление непрерывностью бизнес-процессов и реагирование на инциденты, управление оборудованием и его конфигурацией, шифрование данных, контроль доступа, мониторинг и анализ подключений, сетевую безопасность и ее мониторинг, проведение аудитов.

2.5. Вторая Национальная стратегия кибербезопасности (2019)

Новый документ демонстрирует зрелость национальной политики в области защиты информационного пространства. Он ставит широкий набор целей, достижение которых базируется на 5 компонентах:

1. Обеспечение устойчивой киберзащиты за счет повышения готовности к угрозам всех информационных ресурсов и систем, прежде всего критически важной инфраструктуры.
2. Эффективная государственная система управления рисками и внедрением стандартов информационной безопасности, развитие динамичной экосистемы кибербезопасности.
3. Формирование понимания нацией задач кибербезопасности путем повышения осведомленности, проведения информационных кампаний и программ.
4. Создание системы коллективной обороны от киберугроз в рамках национальной модели партнерства и сотрудничества.
5. Развитие национального кадрового потенциала, повышение уровня подготовки специалистов и руководителей в области кибербезопасности, создание рабочих мест, привлечение талантов и удержание их для долгосрочной карьеры.

По-прежнему актуальными задачами являются развитие законодательной и нормативной базы, повышение доверия к общедоступным онлайн-системам и поощрение их использования, укрепление международного сотрудничества для противодействия киберугрозам.

2.6. Политика Бахрейна в области открытых данных

Еще в 2005 году Управлением ГИС Центральной организации информатики Королевства Бахрейн была внедрена Национальная инфраструктура пространственных данных (NSDI) для открытого доступа к ней государственного и частного сектора, академических учреждений. В настоящее время Портал открытых данных Бахрейна предоставляет многоотраслевые правительственные данные без каких-либо ограничений для повторного использования, анализа или обмена при соблюдении всех правил конфиденциальности персональных данных в соответствии с Законом о защите персональных данных, что стимулирует исследовательские и бизнес-сообщества к разработке и внедрению новых технологических решений на основе анализа Больших данных с использованием искусственного интеллекта.

2.7. Национальная стратегия блокчейн

Королевство Бахрейн относится к числу нескольких передовых государств, которые разработали национальную стратегию использования этой технологии в государственном и частном секторах. Ее авторами стали Совет по экономиче-

скому развитию и Агентство по информации и электронному правительству. Среди внедренных проектов можно отметить регистрацию транспортных средств на блокчейне в Главном управлении дорожного движения, выдачу академических цифровых сертификатов об образовании Университетом Бахрейна.

3. Законодательство в сфере информационной безопасности

Бахрейн был первой страной в Персидском заливе, которая упростила регулирование телекоммуникационного сектора. Введение более гибких правовых рамок способствовало повышению устойчивости ведения бизнеса с использованием ИКТ, повышению информационной безопасности и защиты пользователей, что привело к притоку инвестиций и развитию инноваций. В настоящее время Бахрейн считается одной из благоприятных зон ведения ИКТ-бизнеса.

Основу защиты прав пользователей составляют положения Конституции Королевства Бахрейн (2002) о защите данных, конфиденциальности и свободе электронного общения. В 2018 году был принят Закон № 30 о защите персональных данных, который установил порядок доступа и использования информации физических лиц.

Правила оборота электронных документов и применения цифровых подписей определяются Законом № 54 от 2018 г. о выдаче писем и электронных транзакциях и Постановлением премьер-министра № 36 от 2018 году, регулирующим технические требования к отправке, получению и обновлению электронных записей и подписей государственных органов.

Требования обеспечения информационной безопасности устанавливаются Законом № 16 от 2014 г. о защите государственной информации и документов.

Борьба с киберпреступностью осуществляется на основе Закона № 60 от 2014 г. об ИТ-преступлениях, во многом созвучного Будапештской конвенции. Закон криминализирует незаконный доступ, вмешательство в данные, незаконный перехват и несанкционированное использование устройств, а также преступления, связанные с мошенничеством и детской порнографией. Также он определяет процедурные полномочия, касающиеся перечисленных выше преступлений, сохранения и обработки данных. Следует отметить, что Бахрейн Законом № 2 от 2017 года ратифицировал Арабскую Конвенцию по борьбе с преступлениями в сфере информационных технологий (2010).

К правовым новациям следует отнести Законодательный указ № 56 от 2018 г. в отношении предоставления услуг облачных вычислений иностранным лицам («Облачный закон»). Он позволяет зарубежным потребителям облачных услуг в Королевстве Бахрейн хранить свои данные в расположенных на его территории центрах обработки данных в рамках так называемого «посольства данных»,

которое гарантирует потребителям сохранение их национального суверенитета над этими данными (т.е. юрисдикцию судов иностранного государства и других компетентных органов)[11].

Королевство стремится стать региональным центром финансовых технологий как в традиционном понимании, так и в соответствии с законами шариата. В октябре 2016 г. Центральным банком создано подразделение по финансовым технологиям (финтеху) и инновациям, которое разработало правила регуляторной «песочницы» для тестирования новых финтех-решений. Для участия в программе отобрано 36 компаний, некоторые из которых уже получили разрешения на внедрение своих продуктов.

Кроме того, Центральный банк Бахрейна провел несколько важных нормативных реформ, направленных на защиту рынков капитала от нарушений кибербезопасности в сфере передовых финансовых технологий. Бахрейн первый на Ближнем Востоке ввел лицензирование деятельности для операций с криптоактивами, требования по управлению рисками, борьбе с отмыванием денег и финансированием терроризма, правила делового поведения, отчетности и кибербезопасности. В стране создана лицензированная Центральным банком криптовалютная биржа.

4. Основные угрозы информационной безопасности и общие подходы к противодействию этим угрозам, в том числе основные направления обеспечения информационной безопасности, включая используемые ключевые институты и инструменты защиты

В 2011 году всплеск хактивизма и широкое использование киберпространства страны для разжигания общественных протестов в Бахрейне было оценено как одна из главных угроз информационной безопасности страны, поэтому контроль за контентом очень строгий.

В 2012 компьютерная атака Shamoon против саудовской компании Saudi Aramco и катарской компании RasGas затронула нефтедобывающие предприятия Бахрейна и способствовала усилению мер информационной безопасности национальных критических инфраструктур, которых выделено семь: 1) финансовый сектор; 2) государственные службы и учреждения; 3) здравоохранение; 4) информационные и коммуникационные технологии; 5) транспорт; 6) добыча, переработка и транспортировка газа, электроэнергии и нефти; 7) критически важные производства. Тем не менее, в 2019 году были взломаны защищенные информационные системы Национального агентства безопасности, МВД и офиса заме-

11 Впервые эта правовая концепция введена в рамках двустороннего соглашения между правительствами Эстонии и Люксембурга в 2017 году.

стителя премьер-министра Бахрейна. В июле того же года было зафиксировано вторжение в информационные системы Агентства по электро- и водоснабжению, которое привело к блокировке некоторых функций.

В связи с реализацией государством крупных программ информатизации, в том числе введения цифрового удостоверения личности, перевода государственных структур в облачные сервисы и использования передовых технологий, угрозы информационной безопасности значительно возросли. Всем им уделяется пристальное внимание.

Стратегией кибербезопасности предусмотрены превентивные меры по снижению угроз путем повышения устойчивости государственных информационных ресурсов и систем к компьютерным атакам, развития государственно-частного партнерства в области кибербезопасности, осуществления своевременного информирования частного сектора об угрозах и рассылки рекомендаций по их устранению, проведения кампаний и программ повышения осведомленности в сфере информационной безопасности среди рядовых пользователей. Кроме того, выстроена развитая система защиты национального информационного пространства.

5. Государственные органы, входящие в систему обеспечения информационной безопасности

5.1. Национальный центр кибербезопасности МВД Бахрейна

Головным ведомством по реализации Стратегии кибербезопасности Бахрейна является Министерство внутренних дел.

В 2004 году в министерстве было создано Главное управление по борьбе с коррупцией, экономической и электронной безопасности[12], которое отвечало за расследование преступлений в сфере высоких технологий, а также обеспечение кибербезопасности и разработку систем безопасности для критически важных секторов экономики, включая энергетику, финансы и банковское дело, здравоохранение, образование и др.

В 2014 году в соответствии с решением № 37-2/2013 Высшего совета Бахрейна по информационно-коммуникационным технологиям в структуре управления была создана национальная группа реагирования на компьютерные инциденты (CERT.bh), а в 2017 году для решения задач, связанных с реализацией Стратегии, создан Национальный центр кибербезопасности. В связи с ростом значимости решаемых им задач и необходимостью укрепления вертикали власти в 2020 году

12 В подчинении Главного управления находились Управление по борьбе с коррупционными преступлениями, Управление по борьбе с киберпреступностью, Управление по борьбе с экономическими преступлениями, Управление по международным делам и Интерполу, Управление обнаружения систем вторжения.

Королевским указом № 65/2020 осуществлено переподчинение Национального центра кибербезопасности непосредственно министру внутренних дел.

Генеральный директор центра кибербезопасности в ранге замминистра руководит деятельностью Управления киберполитики, Директората по координации и анализу, Управления поддержки и компьютерных операций, Директората по разработке систем безопасности, Управления контроля и образования. Заместитель генерального директора (в ранге помощника заместителя министра) отвечает за деятельность Директората киберзащиты и Управления национального реагирования.

Такое переподчинение свидетельствует об оптимизации государственного управления в части разделения функций защиты национального киберпространства и борьбы с киберпреступностью, а также повышения оперативности принятия решений в случае необходимости реагирования на значимые компьютерные инциденты.

5.2. Агентство по информации и электронному правительству (IgA)

Агентство выполняет функцию посредника между государственными ведомствами и провайдерами ИКТ-услуг, обеспечивая требуемый уровень безопасности при информатизации государственного сектора, переводе его ресурсов в облако, а также руководит разработкой и предоставлением цифровых услуг населению.

Также в его функции входит подготовка предложений для совершенствования государственной политики, законодательства, программ электронного правительства, укрепления информационной безопасности национального киберпространства. В частности, Агентством разработаны шесть стратегий кибербезопасности для критически важных секторов: государственного управления, здравоохранения, ИКТ, транспорта, сектора газа, электроэнергии и нефти, критической промышленности.

В рамках реализации общенациональной политики «Сначала облако» Агентство разработало ряд политик безопасности, которым должны следовать организации государственного и частного секторов: правила размещения данных в облаке, безопасности паролей, классификации правительственных данных использования беспроводных технологий, правила закупок ИКТ и др.

Агентство имеет соглашение о стратегическом партнерстве с Департаментом развития электронного правительства ООН и раз в два года участвует в обзоре развития электронного правительства, демонстрируя очень высокие результаты.

5.3. Агентство по регулированию телекоммуникаций (TRA)

Агентство создано в 2002 году на основании Закона о телекоммуникациях № 48. Его основной задачей является реализация инициатив, которые укрепляют

сотрудничество между государственным и частным секторами, обеспечивая устойчивость и безопасность ИКТ-услуг в интересах надежной цифровой экономики.

Агентство разработало Целевую рамочную стратегию, согласно которой оно обязуется поощрять и развивать инициативы:

- в области конкуренции в рамках сектора электросвязи;
- внедрению новейших технологий;
- по расширению прав и возможностей потребителей;
- в области широкополосной связи для предоставления высокого качества и по конкурентоспособным ценам;
- в области безопасности и кибербезопасности, которые поддерживают надежную и защищенную ИКТ-инфраструктуру;
- по адаптации нормативно-правовых актов в области электросвязи.

В настоящее время агентство завершает разработку Стратегии кибербезопасности телекоммуникационного сектора, повышающей устойчивость инфраструктуры Королевства.

5.4. Министерство транспорта и телекоммуникаций Бахрейна (МТТ)

Министерство отвечает за реализацию национальных планов в области развития электросвязи и других стратегий, обеспечивает развитие ИКТ-инфраструктуры и предоставление телекоммуникационных услуг, разрабатывает нормативную и правовую базу, общую политику функционирования сектора. Осуществляет международное сотрудничество и участие в работе МСЭ.

5.5. Участие Сил обороны Королевства Бахрейн в обеспечении кибербезопасности

Силы обороны созданы в 1968 году в составе: Королевские ВВС, Королевская гвардия и Королевский ВМФ Бахрейна общей численностью 18 тыс. человек. В функции Сил обороны входят киберзащита и сотрудничество с региональными и международными партнерами в обеспечении безопасности. По данным 2013 года, вооруженные силы Бахрейна принимали участие в программе создания «киберщиты» ССАГПЗ и различных учениях с отработкой задач обеспечения информационной безопасности. Стратегией развития Сил обороны Бахрейна на период до 2030 года создаются киберподразделения в составе Сухопутных войск. В целях централизованного управления системой кибербезопасности Королевства до конца 2022 года предусматривалось сформировать Национальный комитет по кибербезопасности. В настоящее время данные о развитии этой деятельности в открытом доступе отсутствуют.

5.6. Национальный институт стандартов и технологий (NIST)

Бахрейн является единственным государством-членом ЛАГ, имеющей национальный орган стандартизации, что говорит о высоком уровне научной проработки технических стандартов в этой области и участии государства в профильных международных организациях.

6. Участие в международном сотрудничестве в области формирования системы обеспечения международной информационной безопасности в рамках ООН и позиция при голосовании по наиболее важным резолюциям ГА ООН

Бахрейн поддержал создание РГОС, согласно резолюции Генеральной Ассамблеи ООН A/RES/73/27 от 5 декабря 2018 г. и одобрил созыв новой РГОС на 2021–2025 гг. (резолюция Генеральной Ассамблеи ООН A/RES/75/240 от 31 декабря 2020 г.). Однако он воздержался при голосовании за учреждение специального межправительственного комитета экспертов открытого состава для разработки всеобъемлющей международной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях (резолюция Генеральной Ассамблеи ООН A/RES/74/247 от 27 декабря 2019 г.).

7. Участие в международном сотрудничестве с другими международными организациями в области формирования системы обеспечения информационной безопасности на региональном уровне

7.1. Глобальный альянс ООН по ИКТ в целях развития (UN-GAID)

В 2010 году Бахрейн стал членом Стратегического совета UN-GAID, в сотрудничестве было представлено предложение по созданию Центра Целей устойчивого развития и проведения программы наращивания потенциала для обеспечения консультационных услуг в области ИКТ странам Африки и другим наименее развитым странам.

7.2. МСЭ

Государство является членом МСЭ с 1974 года. С учетом достигнутых выдающихся результатов в информатизации страны и развитии электронного правительства в 2022 году Королевство Бахрейн избрано в Совет МСЭ на 2023–2026 годы.

7.3. Совет сотрудничества арабских государств Персидского залива (ССАГПЗ)

Бахрейн является активным членом Исполнительного комитета ССАГПЗ по электронному правительству и находится в постоянном сотрудничестве с его чле-

нами в части разработки Стратегии электронного правительства ССАГПЗ и Плана ее реализации. В 2021 году на 23-м заседании Исполнительного комитета были рассмотрены результаты работы Комитета национальных центров реагирования на компьютерные чрезвычайные ситуации, целевой группы по инфраструктуре открытых ключей (PKI) и целевой группы по унифицированным закупкам программного и аппаратного обеспечения. Комитет также обсудил предложение о создании целевой группы по искусственному интеллекту и другим передовым технологиям.

8. Содержание и оценка предложений и инициатив в области формирования системы обеспечения международной информационной безопасности

Результаты анализа данных открытых источников показывают, что Королевство Бахрейн очень взвешенно подходит к выбору партнеров по сотрудничеству в области региональной и международной информационной безопасности — правовые договоры отсутствуют, при этом для повышения политического авторитета используются инструменты «мягкой силы» — заключение меморандумов, проведение крупных тематических конференций, демонстрация собственных достижений в области кибербезопасности.

В марте 2021 г. в Манаме проведена Международная конференция по использованию искусственного интеллекта в юридической системе с участием экспертов из Саудовской Аравии, Германии, Франции, Бельгии и Королевство, которая дала возможность ознакомить общественность с наработками Бахрейна в указанной сфере. В конце 2021 г. в Манаме проведен Симпозиум критических информационных инфраструктур Юго-Западной Азии.

В декабре 2022 г. Бахрейн провел крупнейший в регионе Арабский международный саммит по кибербезопасности под девизом «Укрепление глобальной кооперации в кибербезопасности». В обсуждении и разработке стратегий защиты ИКТ-инфраструктуры приняли участие государственные органы, профессионалы отрасли и поставщики решений безопасности, представители критически важных отраслей промышленности.

В 2021 году Бахрейн и Саудовская Аравия подписали Меморандум о сотрудничестве в области кибербезопасности в целях укрепления двустороннего взаимодействия и повышения потенциала в сфере борьбы с киберугрозами, а также действий в рамках Исполнительной программы по стандартизации.

В 2022 году Национальный центр кибербезопасности МВД Бахрейна и Совет кибербезопасности ОАЭ подписали Меморандум о взаимопонимании, в соответствии с которым страны будут обмениваться информацией о рисках кибербезопасности и реагировании на инциденты информационной безопасности. Они

также будут обмениваться образовательными и учебными программами по информационной безопасности и повышению осведомленности.

В октябре 2022 г. Бахрейн принял участие в саммите ШОС и запросил статус партнера по диалогу, который уже имеют Катар и Саудовская Аравия.

Результаты проведенного анализа показывают, что Королевство Бахрейн имеет высокоразвитую информационно-коммуникационную инфраструктуру, которую активно применяет для цифровизации экономики. Государство определяет кибербезопасность как ключевой фактор устойчивого развития и комплексно развивает национальную политику в этой сфере. Система защиты национального киберпространства хорошо развита, однако ее уязвимым местом является существенная зависимость от американских поставщиков ИКТ.

3. ДЖИБУТИ

Официальное название: Республика Джибути

Столица: Джибути

Официальные языки: арабский и французский

Территория: 23 200 км² (146-я в мире). Общая длина государственной границы составляет — 508 км, с Эритреей — 113 км, с Эфиопией — 337 км и с Сомали — 58 км. Береговая линия страны: 314 км. Омывается водами бассейна Индийского океана (Аденский залив, Таджурский залив, Баб-эль-Мандебский пролив). Самая высокая точка — гора Мусса-Али — 2028 м.

Горные массивы чередуются с лавовыми плато, с конусами потухших вулканов. В Великой рифтовой долине находится фумарольное поле Боина. Центральную часть страны занимают каменистые, песчаные или глинистые равнины, наиболее пониженные участки которых занимают соленые озера.

Население: 974 000 чел. (по оценкам на 2019 год), что является 160-м показателем в мире.

Государственное устройство: Джибути — республика. В 1896–1946 годах — колония Французское Сомали. С 1946 года — заморская территория Франции. В 1967 году территория получила внутреннее самоуправление и стала называться Французская территория афаров и исса (ФТАИ). 8 мая 1977 г. состоялся референдум, в ходе которого большинство населения высказалось за провозглашение независимости страны. 27 июня 1977 г. провозглашена независимость. Государство получило название Республика Джибути. В стране действует конституция, одобренная на референдуме 4 сентября и вступившая в силу 15 сентября 1992 г.

Глава государства — президент. Он избирается в ходе всеобщего голосования сроком на 6 лет и может переизбираться еще на один срок. Президент имеет серьезное влияние на правительство и является Верховным Главнокомандующим Вооруженных сил Джибути.

Законодательная власть принадлежит однопалатному парламенту — Национальному собранию, который состоит из 65 депутатов. Депутаты избираются всеобщим голосованием сроком на 5 лет.

Исполнительная власть осуществляется президентом и правительством (Совет Министров). Правительство возглавляется премьер-министром. Однако

в стране преобладает клановая общественная иерархия, в результате чего эти группы представителей пытаются овладеть ключевыми постами в исполнительной сфере и поставить на должность премьер-министра ключевую персону определенного клана.

Судебная система основывается на современном праве, мусульманском и традиционном (обычном) праве. Судебную власть представляет Верховный суд, основанный в 1979 году. Есть также Высший апелляционный суд и суд первой инстанции, трибунал безопасности, суды шариата, уголовные суды округов, а также суды по проблемам труда.

Экономика: Показатели ВВП (Паритет покупательной способности) за 2018 год:

- Итого: $5,120 млрд (166-й показатель в мире)
- На душу населения: $4881 (140-й показатель в мире)

Показатели ВВП (Номинал) за 2018 год:

- Итого: $3,013 млрд (161-й показатель в мире)
- На душу населения: $2872 (142-й показатель в мире)

Дипломатические отношения с Россией (СССР): установлены 3 апреля 1978 г.

1. Уровень развития системы обеспечения информационной безопасности и информационно-коммуникационной инфраструктуры (включая индекс развития ИКТ по оценкам МСЭ и ООН)

По данным МСЭ за 2021 год, Джибути является низко информатизированной страной, уровень проникновения Интернета в настоящее время составляет 54,8%. Интегральный индекс кибербезопасности Джибути, рассчитанный МСЭ с учетом развития правовой системы обеспечения информационной безопасности, технических и организационных мер, реализации программ наращивания потенциала и участия в международном сотрудничестве, в 2021 году составил всего лишь 1,73 (из 100), что свидетельствует об отсталости страны в данном вопросе. В глобальном рейтинге кибербезопасности Джибути занимает 179-ю позицию и 21-ю позицию в ЛАГ.

Исходя из приведенных, уровень развития системы информационной безопасности Джибути может быть оценен как очень низкий:

2. Основные документы стратегического планирования в области обеспечения информационной безопасности

Национальная стратегия кибербезопасности имеется только информация о начале ее разработки в 2019 году.

3. Основные угрозы информационной безопасности и общие подходы к противодействию этим угрозам, в том числе основные направления обеспечения информационной безопасности, включая используемые ключевые институты и инструменты защиты

<u>В качестве основных угроз рассматриваются</u>:

- ✓ киберпреступность;
- ✓ угрозы информационной инфраструктуре предприятий и всей стратегической инфраструктуре государства;
- ✓ угрозы надежности и безопасности использования ИКТ.

<u>Особенности обеспечения кибербезопасности и развития ИКТ</u>:

Джибути имеет наибольшее количество международных подводных кабельных соединений в Восточной Африке (подключена к восьми подводным кабелям, соединяющим ее с Европой, Восточной Африкой, Ближним Востоком, восточным Средиземноморьем и Южной Азией), что обусловливает стремление государства стать континентальным центром телекоммуникаций.

Национальное агентство государственных информационных систем (ANSIE) создано в 2015 году в целях содействия кибербезопасности Джибути, для защиты государственной инфраструктуры во всех областях.

Основные задачи:

- ✓ объединение всех администраций страны через широкополосную сеть;
- ✓ разработка сквозных IT-приложений для размещения их в едином центре обработки данных для повышения эффективности и администрирования;
- ✓ развитие онлайн-услуг для граждан, а также отраслевых проектов в области электронного здравоохранения, электронного образования и электронной коммерции.

4. Участие в международном сотрудничестве в области формирования системы обеспечения международной информационной безопасности в рамках ООН и позиция при голосовании по наиболее важным резолюциям ГА ООН

Джибути в целом поддерживает российские инициативы в области международной информационной безопасности.

В 2018–2020 годах проголосовала за принятие российских проектов резолюций Генеральной Ассамблеи ООН:

A/RES/73/27 от 5 декабря 2018 г. (принятие правил, норм и принципов ответственного поведения, а также создание Рабочей группы ООН открытого состава);

A/RES/75/240 от 31 декабря 2020 г. (создание новой Рабочей группы ООН открытого состава по вопросам безопасности в сфере использования ИКТ и самих ИКТ 2021–2025).

Вместе с тем воздержалась при голосовании по российским проектам резолюций Генеральной Ассамблеи ООН:

A/RES/73/187 от 17 декабря 2018 г. (включение в повестку дня ООН обсуждения вопроса о противодействии использованию ИКТ в преступных целях);

A/RES/74/247 от 27 декабря 2019 г. (создание специального межправительственного комитета экспертов открытого состава для разработки всеобъемлющей международной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях).

Джибути проголосовала за принятие американского проекта резолюции Генеральной Ассамблеи ООН A/RES/73/266 от 22 декабря 2018 г. (о создании Группы правительственных экспертов ООН на 2019–2021 годы).

5. Участие в международном сотрудничестве с другими международными организациями в области формирования системы обеспечения информационной безопасности на региональном уровне

Джибути взаимодействует на глобальном и региональном уровнях по вопросам обеспечения кибербезопасности в рамках следующих международных организаций, членом которых она является:

ООН;

ITU (МСЭ);

Движение неприсоединения;

Африканский союз;

ЛАГ;

Интерпол.

6. Содержание и оценка предложений и инициатив в области формирования системы обеспечения международной информационной безопасности

Джибути:

не присоединилась к инициативе Франции — Парижский призыв к доверию и безопасности в киберпространстве (2018 год);

не стала соавтором инициативы Франции и Египта — Программа действий ООН по продвижению ответственного поведения государств в киберпространстве (2020 год).

4. ЕГИПЕТ

Официальное название: Арабская Республика Египет

Столица: Каир

Официальный язык: арабский

Территория: 1 001 450 км² (29-я в мире). Египет граничит на западе с Ливией, на юге — с Суданом, на востоке — с Палестинской автономией и Израилем. Также имеет морскую границу с Саудовской Аравией и Иорданией.

На севере омывается Средиземным морем, на востоке — Красным морем. Египту принадлежит самый крупный рукотворный канал — Суэцкий, который соединяет Средиземное и Красное моря, открывая наиболее короткий путь из Атлантического в Индийский океан.

По всей территории Египта с юга на север протекает река Нил — одна из двух величайших по протяженности рек в мире.

Население: 111 390 203 чел. (по оценкам на 2022 год), что является 14-м показателем в мире.

Государственное устройство: Египет по форме правления является республикой. Глава государства — президент, который одновременно является и главнокомандующим вооруженными силами. Глава правительства — премьер-министр. Высший законодательный орган — двухпалатное Национальное собрание. Нижняя палата парламента, Народная ассамблея (Меджлис Аш-Шааб), состоит из 518 депутатов, 508 из которых избираются по мажоритарной системе, а 10 назначаются президентом. В Народной ассамблее имеются квоты для рабочих и крестьян, а также для женщин.

Экономика: Показатели ВВП (Паритет покупательной способности) за 2019 год:

- Итого: $1,231 трлн (22-й показатель в мире)
- На душу населения: $11 798 (103-й показатель в мире)

Показатели Валового внутреннего продукта (ВВП) (Номинал) за 2019 год:

- Итого: $302,335 млрд (43-й показатель в мире)
- На душу населения: $2577 (133-й показатель в мире)

Дипломатические отношения с Россией (СССР): установлены 26 августа 1943 г.

1. Уровень развития системы обеспечения информационной безопасности и информационно-коммуникационной инфраструктуры (включая индекс развития ИКТ по оценкам МСЭ и ООН)

Египет проводит наиболее успешную политику в цифровой среде среди государств континента.

Важным событием в ЛАГ явилось проведение Египтом в Каире Первой конференции по информационной безопасности и кибербезопасности «CAISEC-22», в которой приняло участие большое количество иностранных IT-компаний.

В период с 19 по 21 июня 2023 г. планируется проведение Первой египетской международной конференции и выставки по безопасности «EISE 2023».

Египет занимает первое место среди арабских стран по количеству владельцев криптовалюты (более 1,7 млн. человек, что составляет 1,8% от численности населения страны).

Согласно прогнозам рынок кибербезопасности Египта будет расти в среднем на 10,7% до 2026 года.

По данным МСЭ за 2021 год, Египет имеет очень высокий индекс кибербезопасности (95,48 из 100) и занимает достаточно высокие позиции как в глобальном рейтинге, где он находится на 23-м месте, так и в рейтинге среди государств-членов ЛАГ, входя в верхнюю четверку по этому показателю.

При этом уровень проникновения Интернета в стране в настоящее время составляет 52,5%.

В соответствии с данными NCSI уровень цифрового развития равняется показателю в 46,93, а индекс готовности к киберугрозам и реагированию на них достигает показателя в 57,14, что говорит о необходимости проделать работу в целях их улучшения.

Исходя из перечисленных статистических данных, уровень развития системы информационной безопасности Египта может быть оценен как высокий.

2. Основные документы стратегического планирования в области обеспечения информационной безопасности

Национальная стратегия кибербезопасности на 2017–2021 годы

Разработана Министерством связи и информационных технологий Египта в декабре 2018 г. с учетом национальных стратегических целей.

Ключевые цели Стратегии:

- ✓ поддержка национальной безопасности и развитие египетского общества;
- ✓ мониторинг и противодействие возникающим угрозам и будущим вызовам в киберпространстве и цифровом обществе.

Основные задачи:

- ✓ распределение функций в области обеспечения кибербезопасности между государственными учреждениями, частным сектором, деловыми кругами и гражданским обществом;
- ✓ определение мер, которые должны быть приняты государством для достижения указанных целей.

Стратегия включает в себя план мероприятий, реализация которого направлена на обеспечение перехода к интегрированной цифровой экономике, определяющей права граждан на комплексное развитие, защищающей благосостояние граждан и национальные интересы.

Национальная стратегия цифрового контента

Разработана Министерством связи и информационных технологий Египта в ноябре 2014 г.

Цели Стратегии:

- ✓ создание благоприятной среды, способствующей продвижению различных видов цифрового арабского контента в соответствии с международными стандартами;
- ✓ формирование необходимой нормативно-правовой базы, включая разработку проектов закона о свободе доступа к данным и информации и закона о кибербезопасности.

Ключевые направления выполнения мероприятий в рамках реализации Стратегии:

- ✓ развитие комплексной и интегрированной инфраструктуры;
- ✓ развитие человеческого капитала, а также институционального потенциала;
- ✓ продвижение государственного контента;
- ✓ продвижение арабского контента;
- ✓ обеспечение устойчивости, включая развитие международного сотрудничества.

Закон о борьбе с киберпреступлениями и технологическими преступлениями (опубликован 19 августа 2018 г.).

Цели Закона:

- ✓ регламентирует меры противодействия экстремистским и террористическим организациям, использующим сеть Интернет для целей продвижения собственных идей среди молодежи;
- ✓ устанавливает запрет на распространение информации о передвижении сил полиции и действующей армии страны;

- ✓ предусматривает уголовную ответственность за осуществление взлома информационных систем (за каждую попытку умышленного взлома информационных систем для целей удаления, изменения, копирования или повторного опубликования данных или информации, содержащихся в указанной системе (сети), предусмотрено наказание в виде лишения свободы на срок на 1 год и штраф от 50 тыс. до 100 тыс. египетских фунтов).

3. Основные угрозы информационной безопасности и общие подходы к противодействию этим угрозам, в том числе основные направления обеспечения информационной безопасности, включая используемые ключевые институты и инструменты защиты

Национальная стратегия кибербезопасности определяет перечень вызовов и угроз в сфере обеспечения кибербезопасности:

- ✓ Угроза саботажа критической инфраструктуры ИКТ (кибератаки, включающие в себя применение вредоносных программ и вирусов). В стратегии уделяется внимание принятию превентивных мер относительно кибератак, осуществляемых параллельно через несколько каналов, включая беспроводные сети, мобильные сети и общие каналы, в том числе электронную почту, веб-сайты, социальные и телекоммуникационные сети.
- ✓ Угроза кибертерроризма и кибервойны. В Стратегии выделяется возможность увеличения количества инцидентов в киберпространстве, организуемых террористическими организациями и международными преступными группировками.

Критическими секторами с точки зрения обеспечения кибербезопасности согласно Национальной стратегии кибербезопасности являются:

- ✓ сектор ИКТ (телекоммуникационные сети, подводные и наземные кабели, башни связи, спутники связи, центры управления связью, телекоммуникационные и Интернет-провайдеры);
- ✓ сектор финансовых услуг (информационные сети и веб-сайты банков, банковские операции, электронные платежные платформы, фондовая биржа, компании по торговле ценными бумагами и почтовые финансовые услуги);
- ✓ энергетический сектор (системы, сети и станции, контролирующие производство и распределение электроэнергии, нефти и газа; высоковольтные плотинные станции; атомные электростанции);
- ✓ транспортный сектор (воздушный, наземный, морской и речной транспорт; системы управления поездами и метро, центры и сети, а также

воздушные и морские навигационные транспортные сети и системы управления);

- ✓ сектор услуг в области здравоохранения и чрезвычайной помощи (сети оказания чрезвычайной помощи, банки крови, больничные системы и сети здравоохранения);
- ✓ сектор информации и культуры (сети, системы и веб-сайты информационных и радиовещательных служб).

Согласно положениям Национальной стратегии кибербезопасности кража цифровых идентификационных данных является одним из самых серьезных преступлений, которые угрожают пользователям Интернета и развитию электронных услуг.

Органы управления и обеспечения в области кибербезопасности

- Высший совет кибербезопасности Египта — главный государственный орган, координирующий деятельность в области кибербезопасности, подотчетный Кабинету министров и возглавляемый Министром связи и информационных технологий.
- Министерство связи и информационных технологий Египта.
- Центр инновационных технологий и предпринимательства — на его базе реализуется программа InnovEgypt, ориентированная на повышение качества знаний и компетенций студентов университетов в технологическом предпринимательстве.

Данная образовательная программа состоит из трех модулей:

- ✓ управление инновациями и технологиями — двухдневный интерактивный курс по управлению инновациями и технологиями;
- ✓ Ideation Camp — двухдневный лагерь для обучения методам мозгового штурма с целью генерирования инновационных идей для преодоления проблем;
- ✓ Entrepreneurship 101 — двухдневный модуль, который охватывает основные концепции предпринимательства и обеспечивает всестороннюю подготовку по ключевым инструментам, необходимым потенциальным предпринимателям для начала нового бизнеса.

Отдельное внимание в рамках указанных курсов уделяется вопросам обеспечения кибербезопасности: в программах выделяются аспекты необходимости соответствия положениям Национальной стратегии кибербезопасности, а также соответствующим международным стандартам.

- Египетская группа по обеспечению готовности к чрезвычайным компьютерным ситуациям (EG-CERT) — команда из 40 штатных специалистов, обеспечивающая круглосуточную поддержку защиты критически важной информационной инфраструктуры (создана Национальным регулирующим органом в области электросвязи).

Основные задачи EG-CERT:

- ✓ обеспечение реагирования на инциденты в области сетевой безопасности;
- ✓ поддержка защиты и анализ кибератак;
- ✓ сотрудничество с государственными, финансовыми учреждениями и любыми другими важнейшими секторами информационной инфраструктуры;
- ✓ обеспечение раннего предупреждения о распространении вредоносных программ и массовых кибератак на телекоммуникационную инфраструктуру Египта.

- Специальный департамент по борьбе с киберпреступностью (создан в 2017 году на базе Главного управления информации и документации Министерства внутренних дел).

Департаментом установлена «горячая линия» для сообщений о киберинцидентах, которые рассматриваются в условиях полной конфиденциальности.

Сотрудники департамента обучаются на курсах по новейшим механизмам борьбы с киберпреступностью в рамках учебной программы «Риски, связанные с небезопасным использованием Интернета» (дополнительная программа для сотрудников всех институтов безопасности).

- Организация информационного противоборства в Египте возложена на Вооруженные силы, где основным органом стратегического планирования этой деятельностью определено Управление военной разведки и контрразведки. Задачи по воздействию на объекты критически важной информационной инфраструктуры могут решаться командованием войск специального назначения, в том числе 777 антитеррористической группой и 999 группой специальных операций.

Национальный телекоммуникационный институт.

В Египте принят свод правил по управлению информационной безопасностью:

- ✓ Кибербезопасность в процессе работы.

Цель — снизить риск человеческой ошибки, кражи, мошенничества или неправильного использования оборудования.

- ✓ Обучение пользователей сети Интернет.

Цель — обеспечить, чтобы пользователи знали об угрозах и проблемах информационной безопасности, были обучены процедурам безопасности и правильному использованию обработки информации средства для минимизации возможных рисков безопасности.

- ✓ Реагирование на инциденты в области информационной безопасности в условиях корпоративной сети.

Цель — свести к минимуму ущерб от сбоев в работе системы безопасности и контролировать данные инциденты, быстро сообщать по соответствующим каналам управления об инцидентах, влияющих на безопасность.

Отдельное внимание на государственном уровне уделяется вопросам безопасности детей в сети Интернет.

4. Участие в международном сотрудничестве в области формирования системы обеспечения международной информационной безопасности в рамках ООН и позиция при голосовании по наиболее важным резолюциям ГА ООН

Египет поддерживает российские инициативы в области международной информационной безопасности, всегда выступая в их поддержку.

В 2018–2020 годах Египет голосовал в поддержку российских проектов резолюций Генеральной Ассамблеи ООН:

- A/RES/73/27 от 5 декабря 2018 г. (принятие правил, норм и принципов ответственного поведения, а также создание Рабочей группы ООН открытого состава);
- A/RES/75/240 от 31 декабря 2020 г. (создание новой Рабочей группы ООН открытого состава по вопросам безопасности в сфере использования ИКТ и самих ИКТ 2021–2025).

В этот же период Египет выступил соавтором российских проектов резолюций Генеральной Ассамблеи ООН:

A/RES/73/187 от 17 декабря 2018 г. (включение в повестку дня ООН обсуждения вопроса о противодействии использованию ИКТ в преступных целях);

A/RES/74/247 от 27 декабря 2019 г. (создание специального межправительственного комитета экспертов открытого состава для разработки всеобъемлющей международной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях).

При голосовании за принятие американского проекта резолюции Генеральной Ассамблеи ООН A/RES/73/266 от 22 декабря 2018 г. (о создании Группы правительственных экспертов ООН на 2019–2021 годы) Египет проголосовал против.

5. Участие в международном сотрудничестве с другими международными организациями в области формирования системы обеспечения информационной безопасности на региональном уровне

Египет взаимодействует на глобальном и региональном уровнях по вопросам обеспечения кибербезопасности в рамках следующих международных организаций, членом которых он является:

ООН;
ITU (МСЭ);
Движение неприсоединения;
Африканский союз;
ЛАГ;
Интерпол;
ISO (Международная организация по стандартизации).

Также Египет участвует в работе:
Организации американских государств — в качестве наблюдателя;
ОБСЕ — в качестве партнера.

6. Содержание и оценка предложений и инициатив в области формирования системы обеспечения международной информационной безопасности

Египет стал соавтором инициативы Франции — Программы действий ООН по продвижению ответственного поведения государств в киберпространстве (2020 год), но не присоединился к инициативе Франции — Парижский призыв к доверию и безопасности в киберпространстве (2018 год).

5. ИОРДАНИЯ


Официальное название: Иорданское Хашимитское Королевство

Столица: Амман

Официальный язык: арабский

Территория: 89 400 км² (110-я в мире). Страна расположена на Ближнем Востоке и граничит с Сирией на севере, Ираком на северо-востоке, Саудовской Аравией на востоке и юге, с Израилем и Палестинскими территориями (Западный берег реки Иордан) на западе. Сухопутная граница с вышеуказанными странами составляет 1619 км. Имеются также границы, очерченные Заливом Акаба и Мертвым морем (береговая линия составляет 26 км).

Население: 11 116 515 чел. (по оценкам на 2023 год), что является 82-м показателем в мире.

Государственное устройство: Форма правления Иордании — дуалистическая монархия. Это закреплено в Конституции, принятой 8 января 1952 г. Исключительная власть сосредоточена в руках короля и совета министров. Король подписывает все законы, его право вето может быть преодолено двумя третями голосов обеих палат Национальной Ассамблеи. Он назначает всех судей своими указами, утверждает изменения в Конституцию, объявляет войну и командует вооруженными силами. Совет министров, возглавляемый Премьер-министром, назначается королем, который может освободить от занимаемой должности отдельных министров по запросу Премьер-министра.

Конституция предусматривает три вида судов: гражданские, религиозные и специальные. Административно Иордания разделена на 12 мухафаз, губернаторов которых назначает король. Они являются единственными руководителями всех отделов правления и проектов развития на вверенных им территориях.

Экономика: Показатели ВВП (Паритет покупательной способности) за 2019 год:

- Итого: $106,039 млрд (86-й показатель в мире)
- На душу населения: $10 530 (112-й показатель в мире)

Показатели ВВП (Номинал) за 2019 год:

- Итого: $44,566 млрд (88-й показатель в мире)
- На душу населения: $4426 (111-й показатель в мире)

Дипломатические отношения с Россией (СССР): установлены 21 августа 1963 г.

1. Уровень развития системы обеспечения информационной безопасности и информационно-коммуникационной инфраструктуры (включая индекс развития ИКТ по оценкам МСЭ и ООН)

По данным МСЭ за 2021 год Иордания является высоко информатизированной страной, уровень проникновения Интернета в настоящее время составляет 84,7%. Интегральный индекс кибербезопасности Иордании, рассчитанный МСЭ с учетом развития правовой системы обеспечения информационной безопасности, технических и организационных мер, реализации программ наращивания потенциала и участия в международном сотрудничестве, в 2021 году составил 70,96 (из 100), что существенно выше общемирового показателя. В глобальном рейтинге кибербезопасности Иордания занимает 71-ю позицию, и 10-ю в ЛАГ.

Исходя из перечисленных статистических данных, уровень развития системы информационной безопасности Иордании может быть оценен как высокий.

2. Основные документы стратегического планирования в области обеспечения информационной безопасности

Национальная стратегия обеспечения информационной безопасности и кибербезопасности (NIACSS) принята Правительством Иордании в 2012 году.

Основные приоритеты в области кибербезопасности для правительства, бизнеса и граждан:

- ✓ обеспечить эффективное противодействие угрозам национальной кибербезопасности;
- ✓ наилучшим образом использовать существующие возможности и ресурсы, обеспечивая при этом устойчивый суверенный потенциал за счет развития ресурсов;
- ✓ эффективная и долгосрочная приверженность обеспечению кибербезопасности со стороны правительства, частного сектора и граждан, их взаимодействие и сотрудничество;
- ✓ развитие образования и науки в целях обеспечения безопасности иорданцев в сети Интернет, а также подготовка специалистов защиты национальной информационной безопасности.

Национальная стратегия кибербезопасности на 2018–2023 годы определяет порядок реализации правительством данных приоритетов.

Основное содержание Стратегии:

- ✓ итоги достижения целей, поставленных Стратегией 2012 года;
- ✓ анализ текущих тенденций в области киберугроз;
- ✓ акцент на необходимость более надежного национального подхода к управлению кибербезопасностью;
- ✓ необходимость взаимодействия правительства с гражданами, бизнесом и научными кругами, улучшение координации и правоприменения;
- ✓ необходимость кибербезопасности для успеха цифровой экономики;
- ✓ необходимость мер против распространения «поддельных новостей» злоумышленниками и других элементов информационных операций;
- ✓ обеспечение на самом высоком уровне управления кибербезопасностью.

Руководящие принципы Стратегии:

- ✓ кибербезопасность в качестве главного приоритета противодействия угрозам национальной безопасности будет координироваться на высоком государственном уровне;
- ✓ правительство установит соответствующие уровни национального управления, координации и контроля для обеспечения совместного подхода к развитию кибернетических возможностей, защите, реагированию на кризисы и восстановление после них;
- ✓ применение мер кибербезопасности к организациям и системам будет приоритетным по степени риска и воздействия, поскольку предотвратить все кибератаки невозможно или очень затратно;
- ✓ кибербезопасность — это общая ответственность правительства, бизнеса, научных кругов и отдельных лиц;
- ✓ правительство несет основную ответственность за обеспечение защиты от киберугроз критически важной инфраструктуры, как государственной, так и частной;
- ✓ повышение осведомленности рядовых пользователей сети Интернет в области кибербезопасности;
- ✓ связь с государственной политикой в секторах ИКТ, почтовой связи и ключевыми стратегиями электронного правительства жизненно важна для успеха киберстратегии;
- ✓ позитивная культура кибербезопасности необходима для ее эффективности, а развитие граждан и бизнеса имеет основополагающее значение для успеха возможностей кибербезопасности;
- ✓ управление цифровыми рисками и надлежащее применение кибербезопасности будут входить в обязанности Совета директоров всех компаний;
- ✓ кибербезопасность должна быть включена во все человеческие, физические и технологические решения;

- ✓ глубокая защита и безопасность должны стать основными принципами проектирования сетей и инфраструктуры.

3. Основные угрозы информационной безопасности и общие подходы к противодействию этим угрозам, в том числе основные направления обеспечения информационной безопасности, включая используемые ключевые институты и инструменты защиты

Среди основных киберугроз Иордании и проблем в области обеспечения кибербезопасности выделяются следующие:

- ✓ рост наступательных кибернетических возможностей государств;
- ✓ устремления некоторых государств подорвать региональную и национальную стабильность;
- ✓ деятельность служб внешней разведки путем прямых внешних атак на информационные ресурсы правительств и подрывной деятельности их персонала;
- ✓ кибершпионаж и распространение ложной информации (поддельные новости), используемые некоторыми национальными государствами и другими субъектами в качестве инструментов достижения политических и экономических потрясений;
- ✓ кражи огромных объемов секретных данных из «высокозащищенной» сети инсайдером и их передача СМИ, общественности или иностранным разведывательным службам и другим организациям;
- ✓ обвинения во вмешательстве в демократические процессы;
- ✓ кибератаки на критически важную инфраструктуру (прежде всего, на нефтегазовый сектор, оборону и безопасность, энергетику, транспорт, коммунальные услуги, продовольствие и строительство и другие важнейшие отрасли промышленности) в целях воздействия на системы управления для получения политической или экономической выгоды;
- ✓ стремление террористов к совершению террористических актов с использованием ИКТ на более высоком уровне.
- ✓ хактивизм — использование технических инструментов и средств для получения несанкционированного доступа к компьютерным файлам или сетям для продвижения или демонстрации политических, социальных, идеологических или религиозных идей с помощью незаконных или юридически неоднозначных методов;
- ✓ рост глобальной зависимости от сетей и новых технологий, который провоцирует увеличение возможностей злоумышленников, активизация их усилий и стратегических методов работ;

- ✓ использование небрежности или недовольства людей, приводящих к нарушениям информационной безопасности непреднамеренно или намеренно;
- ✓ использование киберпреступниками скорости, удобства и анонимности сети Интернет для совершения разнообразных преступных действий, которые не знают границ, как физических, так и виртуальных, наносят серьезный вред жертвам во всем мире и представляют реальную угрозу;
- ✓ использование киберпреступниками вирусов-вымогателей (вредоносные программы, способные шифровать или уничтожать файлы);
- ✓ использование искусственного интеллекта для более целенаправленных фишинговых электронных писем и рекламы, создание чат-ботов для получения финансовой информации;
- ✓ распространение фишинговых электронных писем для заражения вредоносными программами или для побуждения жертв разглашать личную информацию;
- ✓ злоумышленное использование недостатков в системах безопасности и конфиденциальности облачных технологий;
- ✓ рост числа наемных хакеров в связи с простотой использования и доступностью инструментов для злоумышленников;
- ✓ недостаточная осведомленность общественности о кибербезопасности;
- ✓ острая нехватка квалифицированных специалистов в области кибербезопасности для государственного и частного секторов.

Национальная программа кибербезопасности (NCP) была разработана для достижения стратегических целей и национальных приоритетов, изложенных в киберстратегии 2012 года (NIACSS).

Основные итоги реализации Программы:

- ✓ завершена программа оценки критических сетевых рисков, основанная на международно-признанных стандартах, активно используются результаты этой работы для повышения безопасности;
- ✓ определен набор стандартов и политик информационной безопасности, необходимых для обеспечения расширенного и последовательного подхода к национальной информационной безопасности;
- ✓ созданы специальные группы реагирования на компьютерные чрезвычайные ситуации (CERTs) для обеспечения непрерывного мониторинга сети, анализа угроз и реагирования на инциденты;
- ✓ проведена программа кибертренинга для повышения квалификации заинтересованных участников программы NCP и сотрудников CERT;

- ✓ создана инфраструктура открытых ключей (PKI) для использования криптографических средств, управления безопасной передачей информации, аутентификацией личности и цифровых подписей;
- ✓ начато создание международной программы сотрудничества в области информационной безопасности для содействия обмену информацией и расширению возможностей.

Национальные приоритеты в области кибербезопасности:

- Национальные стандарты и политика кибербезопасности. Национальный единый подход к кибербезопасности будет поддерживаться публикацией национальных стандартов и политик кибербезопасности в форме Основы политики безопасности и управляться через Национальную комиссию по кибербезопасности;
- Программа международного сотрудничества в области информационной безопасности. Способствует обеспечению готовности надежно защищать информацию и обмениваться ею с иностранными правительствами и организациями;
- Программа повышения осведомленности о безопасности и наращивания потенциала. Служит активизации взаимодействия с научными кругами и международными партнерами, а также накоплению национального опыта;
- Программа защиты критической национальной инфраструктуры (CNIP);
- Национальные группы реагирования на компьютерные инциденты (CERTs). Система таких групп (в правительстве, министерствах обороны, безопасности, финансов, критической национальной инфраструктуры) обеспечивает скоординированный анализ, распространение предупреждений о киберугрозах, реагирование на киберинциденты и поддержку частного сектора;
- Правовая реформа. Проведение законодательной реформы для обеспечения эффективного баланса между национальной безопасностью и конфиденциальностью пользователей.
- Национальная комиссия по кибербезопасности — центр передового опыта в области кибербезопасности, обеспечивающий активную киберзащиту, обнаружение кибератак и реагирование на них, а также выступает связующим звеном между правительством, бизнесом, научными кругами и гражданами в реализации Национальной стратегии кибербезопасности.

Основные задачи Комиссии:

- ✓ сбор и анализ информации из различных источников для информирования об оценке киберугроз и идентификации аномального поведения для расследования и принятия мер;
- ✓ создание надлежащих правовых возможностей для поддержки управления и выполнения всех правовых и нормативных требований, связанных с кибербезопасностью, необходимых для реализации Национальной стратегии кибербезопасности;
- ✓ стратегическое планирование для определения будущих требований, которые могут повлиять на стратегическое направление кибербезопасности, а также тестирование текущих возможностей для обеспечения ожидаемого уровня кибербезопасности или определения областей для улучшения;
- ✓ оценка киберинструментов, продуктов и услуг на предмет их пригодности для использования и разработка новых инструментов и подходов для использования специалистами по всей стране;
- ✓ разработка эффективных рекомендаций и стандартов для всех элементов кибербезопасности;
- ✓ выявление важнейших национальных активов, которым могут угрожать киберинциденты, оказывающие значительное воздействие, и проведение для них оценок рисков с целью определения и реализации приоритетных мер по управлению выявленными рисками;
- ✓ развитие четкого понимания киберсреды, в которой работают организации государственного и частного секторов, для поддержки мер по повышению осведомленности об угрозах и кибербезопасности;
- ✓ предоставление механизмов для сбора и распространения предупреждений о кибератаках среди организаций конечных пользователей, чтобы организации имели как можно больше возможностей для управления последствиями кибератак;
- ✓ определение и внедрение последовательного и эффективного подхода к управлению инцидентами, связанными с киберпространством, для обеспечения того, чтобы организации могли их сдерживать и при необходимости играть ведущую роль;
- ✓ развитие национальных и организационных возможностей для быстрого реагирования на киберинциденты;
- ✓ предоставление технических и криминалистических методов расследования инцидентов, связанных с киберпространством, которые при необходимости могут быть юридически допустимыми;
- ✓ проверка соответствия организации собственным и внешним требованиям кибербезопасности путем оценки соответствия установленным по-

литикам, стандартам и руководящим принципам и предоставления конструктивной обратной связи, направленной на обеспечение улучшения состояния кибербезопасности;

- ✓ определение мер физической безопасности, необходимых для защиты киберактивов от случайных или преднамеренных действий.

4. Участие в международном сотрудничестве в области формирования системы обеспечения международной информационной безопасности в рамках ООН и позиция при голосовании по наиболее важным резолюциям ГА ООН

Следует отметить, что в 2019–2021 Иордания была членом ГПЭ, поддерживает российские инициативы в области международной информационной безопасности, всегда голосуя за их принятие.

В 2018–2020 годах проголосовала в поддержку российских проектов резолюций Генеральной Ассамблеи ООН:

- A/RES/73/27 от 5 декабря 2018 г. (принятие правил, норм и принципов ответственного поведения, а также создание Рабочей группы ООН открытого состава);
- A/RES/73/187 от 17 декабря 2018 г. (включение в повестку дня ООН обсуждения вопроса о противодействии использованию ИКТ в преступных целях);
- A/RES/74/247 от 27 декабря 2019 г. (создание специального межправительственного комитета экспертов открытого состава для разработки всеобъемлющей международной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях);
- A/RES/75/240 от 31 декабря 2020 г. (создание новой Рабочей группы ООН открытого состава по вопросам безопасности в сфере использования ИКТ и самих ИКТ 2021–2025).

Иордания проголосовала за принятие американского проекта резолюции Генеральной Ассамблеи ООН A/RES/73/266 от 22 декабря 2018 г. (о создании Группы правительственных экспертов ООН на 2019–2021 годы).

5. Участие в международном сотрудничестве с другими международными организациями в области формирования системы обеспечения информационной безопасности на региональном уровне

Иордания взаимодействует на глобальном и региональном уровнях по вопросам обеспечения кибербезопасности в рамках следующих международных

организаций, членом которых она является: ООН; МСЭ; Движение неприсоединения; ЛАГ; Международная организация по стандартизации (ISO); Интерпол.

В рамках программы НАТО «Наука ради мира и безопасности» в Королевстве с 2017 года организована работа национальной группы реагирования на компьютерные инциденты (JOCERT) и ее военной составляющей — группы компьютерного противоборства (JAFCERT) в составе Министерства обороны и безопасности.

Основные цели международного сотрудничества:

- ✓ установление соответствующих региональных и международных отношений для эффективного сотрудничества с правительствами и организациями-единомышленниками по вопросам, связанным с кибербезопасностью, с учетом национальных интересов;
- ✓ создание и поддержание прочных международных союзов и партнерских отношений для предотвращения общих угроз и укрепления международной безопасности и стабильности.

Основные задачи по достижению целей сотрудничества:

- ✓ заключение международных и региональных соглашений на самых высоких уровнях государственного управления для сотрудничества в области надлежащего обмена данными киберразведок;
- ✓ заключение международных соглашений, позволяющих Иордании извлекать выгоду из передовых исследований и разработок в области кибербезопасности и вносить в них свой вклад;
- ✓ заключение международных юридических соглашений, позволяющих сотрудничать в целях привлечения киберпреступников к ответственности;
- ✓ влияние и формирование международной и региональной политики, связанной с кибербезопасностью;
- ✓ заключение международных и региональных соглашений о контроле за кибербезопасностью.

6. Содержание и оценка предложений и инициатив в области формирования системы обеспечения международной информационной безопасности

Иордания не присоединилась к инициативе Франции «Парижский призыв к доверию и безопасности в киберпространстве» (2018 год), а также не стала соавтором инициативы Франции и Египта «Программа действий ООН по продвижению ответственного поведения государств в киберпространстве» (2020 год).

6. ИРАК

Официальное название: Республика Ирак

Столица: Багдад

Официальные языки: арабский и курдский

Территория: 437 072 км² (58-я в мире). Расположена на севере Аравийского полуострова и омывается водами Персидского залива. Большая часть Ирака расположена в пределах Месопотамской низменности, являющейся передовым прогибом, разделяющим докембрийскую Аравийскую платформу и молодые нагорья Альпийско-Гималайского подвижного пояса.

Население: 41 310 000 чел. (по оценкам на 2019 год), что является 35-м показателем в мире.

Государственное устройство: Ирак — демократическая, федеративная, парламентская республика, состоящая из 18 провинций.

Президент является главой государства и олицетворением ее единения, носителем суверенитета, гарантом Конституции Республики Ирак.

Наряду с институтом Президентства в исполнительной власти функционирует кабинет Министров. Кабинет Министров формируется Президентом Республики. Также Президентом назначается Премьер-министр, который отвечает за основные направления внешней политики государства, определяет работу Кабинета министров, является главнокомандующим вооруженными силами Республики Ирак.

Федеральная законодательная власть Республики Ирак состоит из Совета Представителей и Совета Федерации. Полномочия Совета Представителей и Совета Федерации разграничены и прописаны в Конституции.

Экономика: Показатели ВВП (Паритет покупательной способности) за 2019 год:

- Итого: $447,867 млрд (48-й показатель в мире)
- На душу населения: $11 450 (110-й показатель в мире)

Показатели ВВП (Номинал) за 2019 год:

- Итого: $230,143 млрд (49-й показатель в мире)
- На душу населения: $5929 (92-й показатель в мире)

Дипломатические отношения с Россией (СССР): на уровне миссий установлены 9 сентября 1944 г.

1. Уровень развития системы обеспечения информационной безопасности и информационно-коммуникационной инфраструктуры (включая индекс развития ИКТ по оценкам МСЭ и ООН)

Исходя из статистических данных, уровень развития системы информационной безопасности Ирака низкий:

МСЭ 2021, индекс кибербезопасности: 20,71 (из 100)

МСЭ 2021, позиция в рейтинге среди государств-членов ЛАГ: 17

МСЭ 2021, позиция в глобальном рейтинге: 129

МСЭ, уровень проникновения Интернет: 91,8%

2. Основные документы стратегического планирования и правового регулирования в области обеспечения информационной безопасности

2.1. Национальная стратегия кибербезопасности Республики Ирак

Утверждение Стратегии состоялось 16 февраля 2022 г. на сессии Совета национальной безопасности во главе с премьер-министром и главнокомандующим вооруженными силами Мустафой аль-Казыми. Совет принял замечания, которые способствуют повышению уровня кибербезопасности в Ираке, подготовленные иракской группой реагирования на киберинциденты (IQ-CERT) и специалистами в этой области.[1]

Национальная стратегия кибербезопасности[2] — это стратегия готовности государства, предусматривающая последовательные меры и стратегические действия для обеспечения безопасности и защиты иракского присутствия в киберпространстве, защиты критически важной информационной инфраструктуры, создания и развития доверенного интернет-сообщества. Она состоит из нескольких краткосрочных, среднесрочных и долгосрочных Стратегий, которые охватывают все угрозы, наносящие ущерб национальной безопасности.

Главная цель этой стратегии — предоставить согласованную дорожную карту, инициативы и механизмы для реализации и достижения национального видения кибербезопасности, оперативной структуры и процедур, которые обеспечивают достижение национального видения и целей, связанных с кибербезопасностью.

Стратегия необходима для достижения следующих конкретных целей:

1) разработать комплексное законодательство по борьбе с киберпреступностью и контрмеры против киберугроз, которые могут быть приняты на

1 https://cert.gov.iq/events.htm

2 https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/00056_06_iraqi-cybersecurity-strategy.pdf

национальном, региональном и глобальном уровнях, актуальные в контексте обеспечения безопасности киберпространства страны;

2) предусмотреть меры, которые защищают критическую информационную инфраструктуру, а также уменьшают уязвимости;
3) разработать эффективный механизм реагирования на чрезвычайные компьютерные ситуации;
4) усилить работу над повышением потенциала Национальной группы реагирования на компьютерные инциденты (Iraq Cyber Events Response Team);
5) создать национальные механизмы по наращиванию потенциала, информированию общественности и расширению навыков, необходимых для повышения способности быстро и эффективно реагировать на компьютерные атаки;
6) разработать надежный механизм коллективного реагирования на киберугрозы с участием многих заинтересованных сторон на национальном и международном уровнях;
7) сдерживать и защищать правительство от всех форм кибератак;
8) координация инициатив по кибербезопасности на всех уровнях власти в стране.

Согласно Стратегии Ирак должен рассматривать область киберпространства как свою четвертую сферу, помимо воды, суши и воздуха, из-за ее эффективного и явного влияния на решение критически важных национальных задач, таких как экономическое развитие, торговля и транзакции, социальное взаимодействие, взаимодействие в области медицины и здравоохранения, правительственные операции и национальная безопасность.

В стратеги указывается, что преступные государственные и негосударственные субъекты в достаточной степени оснащены сложными инструментами для нанесения ущерба беспрецедентного масштаба. Фокус на кибербезопасность поможет стране подготовиться к этим угрозам и ответить на них, поможет устранить уязвимость страны в цифровой среде, а также повысит способность совместно с другими государственными и негосударственными субъектами принимать контрмеры. Это стратегическое обоснование для разработки национальной политики кибербезопасности.

В Стратегии также рассматривается стремление дать возможность нации создать всеобъемлющие возможности, как структурные, так и процедурные, на стратегическом и тактическом уровнях для снижения киберрисков. Критический фактор успеха Стратегии зависит от всесторонней мобилизации, участия и координации критически важных компонентов для обеспечения присутствия в киберпространстве и защиты критически важных информационных инфраструктур.

Направление политики правительства в области кибербезопасности соответствует региональной и глобальной тенденции в области обеспечения безопасности киберпространства. Ключевым направлением Стратегии кибербезопасности является устранение подверженности киберрискам, защита национальной информационной инфраструктуры, использование возможностей киберпространства для достижения целей национальной безопасности и экономики, а также работа по поддержке надежного киберсообщества.

2.2. Закон о борьбе с киберпреступностью

22 января 2013 г. парламентский Комитет по культуре и СМИ подал запрос об отмене Закона о киберпреступности 2010 года[3], проект которого был одобрен спикером Палаты.

Законопроект угрожал интернет-свободам, криминализируя определенные виды высказываний и предусматривая несоразмерные наказания, включая пожизненное заключение за «использование компьютеров для «нанесения вреда репутации» или ущерба «единству» страны».

23 ноября 2020 г. Совет представителей Ирака (парламент) завершил чтение и обсуждение законопроекта о борьбе с киберпреступностью.[4] Законопроект определяет ряд действий, которые классифицируются как киберпреступления, и устанавливает наказания за них. При обсуждении положений законопроекта члены парламента призвали найти баланс между преступлениями, указанными в законопроекте, и соразмерностью наказаний, назначаемых за эти преступления.

Законопроект о борьбе с киберпреступностью состоит из 21 статьи. Закон будет применяться к преступлениям, совершенным на территории Ирака или за рубежом. (Статья 3) Положения этого Закона гарантируют свободу выражения мнений для отдельных лиц, институтов гражданского общества и средств массовой информации при условии, что они выражают свое мнение объективным и конструктивным образом в пределах, установленных Конституцией Ирака (Статья 4).

Законопроект предусматривает определение ряда преступлений и введение уголовных наказаний за них. Например, законопроект предусматривает наказание в виде лишения свободы на срок от одного до трех лет и штрафа в размере от 1 млн. до 3 млн. иракских динаров за взлом любого электронного аккаунта с целью перехвата почтовых сообщений (Статья 5). Законопроект также предусматривает наказание в виде лишения свободы на срок от семи до десяти лет

3 https://www.slideshare.net/SMEXbeirut/ss-8927775

4 https://aliraqnet.net/%D9%86%D8%B5-%D9%82%D8%A7%D9%86%D9%88%D9%86-%D8%AC%D8%B1%D8%A7%D8%A6%D9%85-%D8%A7%D9%84%D9%85%D8%B9%D9%84%D9%88%D9%85%D8%A7%D8%AA%D9%8A%D8%A9-2020-%D8%A7%D9%84%D8%B0%D9%8A-%D8%B3%D9%8A%D8%B6%D8%B9/

и штрафа в размере от 5 до 10 млн. динаров за использование компьютера или системы информационных технологий с целью получения данных, касающихся национальной безопасности Ирака, удаления информации или изменения данных, затрагивающих национальную безопасность Ирака (Статья 5).

Лица, использующие компьютер или информационную систему для получения данных с целью шантажа другого лица, наказываются лишением свободы на срок от трех до пяти лет и штрафом в размере от 5 млн. до 10 млн. динаров (Статья 6).

Законопроект направлен на защиту так называемого «общественного порядка и нравственности». Он предусматривает наказание любого лица, которое использовало компьютер или информационную систему для создания, управления или помощи в создании веб-сайта для продвижения или поощрения безнравственности и разврата или программ, информации, изображений или видео, нарушающих общественные приличия и мораль (Статья 8). Кроме того, законопроект предусматривает наказание в виде лишения свободы на срок от семи до десяти лет и штрафа в размере от 5 млн до 10 млн динаров за использование компьютера или информационной системы для вовлечения другого лица в занятие проституцией.

Законопроект защищает право на неприкосновенность частной жизни, наказывая любое лицо, которое использовало мобильный телефон или информационно-технологическую систему для нарушения неприкосновенности частной жизни другого лица путем фотографирования или публикации аудио- или видеозаписей, связанных с другим лицом, без его согласия (Статья 8).

Наконец, законопроект предусматривает создание государственного органа под названием Национальный центр цифровых доказательств, основной функцией которого будет подготовка отчетов о технических особенностях и типах цифровых данных, используемых для доказательства компьютерных преступлений (Статья 21).

3. Основные угрозы информационной безопасности и общие подходы к противодействию этим угрозам, в том числе основные направления обеспечения информационной безопасности, включая используемые ключевые институты и инструменты защиты

В рассмотренной выше Стратегии кибербезопасности выделяются следующие угрозы:

1) трояны и вирусы;
2) взлом устройства;
3) отказ в обслуживании;

4) нарушение доступа;
5) кража пароля;
6) вторжение в систему;
7) взлом информационного ресурса в сети Интернет;
8) использование частных и общедоступных веб-браузеров;
9) обмен мгновенными сообщениями и злоупотребление СМИ, социальными коммуникациями.

В Стратегии называются источники этих угроз: зарубежные страны, организованные преступные сообщества, террористические и экстремистские группы, хакеры, корпорации.

3.1. Иракская группа реагирования на киберинциденты (ICERT — Iraq Cyber Events Response Team)

Группа[5] специализируется в области кибербезопасности, реагировании на инциденты информационной безопасности, защите интернет-инфраструктуры и распространении информации в области защиты конфиденциальности и самозащиты отдельных лиц и организаций в Интернете.

Команда несет ответственность за обеспечение безопасности и защиту сетей, национальных дата-центров и официальных веб-сайтов, работающих в киберпространстве Ирака, координацию национальных усилий и поддержку учреждений государственного и частного секторов в защите себя и своих услуг в киберпространстве.

Цели группы:

- ✓ реагирование на инциденты безопасности, снижение их последствий и принятие упреждающих мер для предотвращения подобных инцидентов;
- ✓ создание национальных рамок кибербезопасности для поощрения сотрудничества между государственным и частным секторами и обмена информацией;
- ✓ повышение доверия к использованию государственных электронных услуг;
- ✓ повышение осведомленности пользователей систем информационных технологий и Интернета о безопасности;
- ✓ развитие возможностей менеджеров ИТ-систем по обеспечению безопасности в случае инцидентов безопасности;
- ✓ анализ угроз безопасности и их влияния, предоставление информации о последних инцидентах и способах их предотвращения;
- ✓ создание уполномоченного центра по приему сообщений об инцидентах;
- ✓ поощрение исследований и разработок в области кибербезопасности;

5 https://cert.gov.iq/

- ✓ совместное сотрудничество с группами реагирования и организациями на региональном и международном уровнях.

С февраля 2019 г. уполномоченным органом за кибербезопасность Ирака определено Управление информационной безопасности (20 сотрудников), которое подчинено руководителю канцелярии главы правительства и парламенту страны.

4. Участие в международном сотрудничестве в области формирования системы обеспечения международной информационной безопасности в рамках ООН и позиция при голосовании по наиболее важным резолюциям ГА ООН

Ирак поддержал российский проект резолюции Генеральной Ассамблеи ООН A/RES/73/27 о переформатировании дискуссии по МИБ в прозрачный, инклюзивный диалог и созыве РГОС (A/RES/73/27 от 5 декабря 2018 г.).

Резолюция Генеральной Ассамблеи ООН A/RES/73/187 «Противодействие использованию информационно-коммуникационных технологий в преступных целях» от 17 декабря 2018 г. была поддержана.

Ирак одобрил американский проект резолюции Генеральной Ассамблеи ООН «Поощрение ответственного поведения государств в киберпространстве в контексте международной безопасности» (A/RES/73/266 от 22 декабря 2018 г.).

5. Участие в международном сотрудничестве с другими международными организациями в области формирования системы обеспечения информационной безопасности на региональном уровне

5.1. Сотрудничество с НАТО

Иракские эксперты прошли обучение по киберзащите в Ближневосточном техническом университете (METU) в Анкаре (Турция), чтобы увеличить свой опыт, углубить технические навыки и внести вклад в укрепление национального потенциала киберзащиты Ирака. Курс был направлен на повышение осведомленности о кибербезопасности и предоставил слушателям технические знания, которые помогут повысить устойчивость их национальных сетей. Этот курс был организован при поддержке программы «Наука для мира и безопасности» и проходил с 21 ноября по 2 декабря 2016 г.

6. Содержание и оценка предложений и инициатив в области формирования системы обеспечения международной информационной безопасности

Хотя Интернет в Ираке практически свободен и доступ в сеть беспрепятственный, развитие кибербезопасности в стране назрело, а инфраструктура сильно пострадала в результате десятилетий войны. Чтобы повысить информационную безопасность страны, иракским законодателям необходимо укрепить и поддержать инфраструктуру и ИКТ-сектор. Стратегия кибербезопасности на это нацелена и базируется на трех приоритетных задачах: создание более безопасного киберпространства, развитие инфраструктуры, международное партнерство.

7. ЙЕМЕН

Официальное название: Йеменская Республика

Столица: Сана

Официальный язык: арабский

Территория: 527 970 км² (49-я в мире). Йемен расположен на юге Аравийского полуострова. Омывается водами Красного и Аравийского морей, Индийского океана. Имеет сухопутную границу с Оманом (на востоке) и Саудовской Аравией (на севере). Северо-восток Йемена покрыт раскаленной каменистой пустыней, где дожди не выпадают годами.

Население: 32 162 000 чел. (по оценкам на 2020 год), что является 49-м показателем в мире.

Государственное устройство:

Глава государства — президент, избираемый (с 1999 года) прямым всеобщим голосованием на 7 лет.

Законодательная власть представлена двухпалатным парламентом: Шура (Совет) (111 членов, назначаются президентом) и палата представителей (избирается населением на 6-летний срок, 301 депутат).

Экономика: Показатели ВВП (Паритет покупательной способности) за 2019 год:

- Итого: $65,088 млрд (104-й показатель в мире)
- На душу населения: $2057 (174-й показатель в мире)

Показатели ВВП (Номинал) за 2019 год:

- Итого: $22,568 млрд (100-й показатель в мире)
- На душу населения: $713 (168-й показатель в мире)

Дипломатические отношения с Россией (СССР): установлены 1 ноября 1928 г.

1. Уровень развития системы обеспечения информационной безопасности и информационно-коммуникационной инфраструктуры

По данным Всемирного банка до 2015 г. государственные доходы Йемена от ИКТ-отрасли были вторыми по величине после углеводородов. Телекоммуникационные услуги ежегодно приносили в экономику порядка $300 млн. К началу 2016 г. более половины населения было пользователями мобильной связи (16 млн человек). Государственные операторы связи (MTN Yemen и Yemen Mobile) имели лицензии на сети широкополосной мобильной связи 3G, а коммерческие компании с иностранным капиталом — только на сети 2/2,5G. Это привело к тому, что только 1,7% населения имело доступ к услугам мобильного Интернета, который был самым дорогостоящим в регионе и находился под государственным контролем.

Тем не менее развитие телекоммуникационной отрасли было очевидным, объем импорта ИКТ составлял порядка $160 млн. В 2014 году государственная телекоммуникационная корпорация PTC проложила по всей стране магистральную оптоволоконную сеть длиной 13 тыс. км, которая соединила Йемен с точками обмена международным трафиком в трех городах на побережье (Аден, Эль-Макалла, Ходейда), а также с городом Саада на границе с Саудовской Аравией.

В настоящее время развитие ИКТ-отрасли Йемена отброшено далеко назад. Не прекращающаяся с 2014 г. гражданская война и противостояние коалиционным силам арабских государств во главе с Саудовской Аравией сильно ослабили экономику. Инфраструктура разрушается в результате авиаударов и боевых действий. В 2017 г. по данным МСЭ количество индивидуальных пользователей сети Интернет составляло 27% населения, в июле 2022 г. уровень проникновения Интернета (соотношение пользователей сети к населению страны) упал до 25,9%. По данным Всемирного банка, в 2018 году импорт ИКТ достиг своего минимума с 2007 года — $60,3 млн, после чего начался некоторый подъем. Риски частных телекоммуникационных компаний настолько велики, что развитие бизнеса практически остановлено. Уровень платежеспособности крайне низок. По данным ООН, значительная доля населения остро нуждается в гуманитарной помощи из-за критического голода.

В связи отсутствием полноценных статистических данных, МСЭ в 2020 году не смог собрать необходимую информацию для оценки уровня кибербезопасности Йемена и определил ему 182-ю позицию в глобальном рейтинге и последнюю позицию в регионе, хотя в 2015 году государство занимало 13-е место среди государств-членов ЛАГ.

В целом, крайне низкий уровень информационной безопасности соответствует состоянию телекоммуникационной инфраструктуры и экономическому положению страны.

2. Основные документы стратегического планирования в области обеспечения информационной безопасности

2.1. Стратегическое видение телекоммуникационных и информационных технологий в поддержку комплексных планов развития в Йемене (2002–2025 годы)

Основными целями национальной политики в сфере ИКТ являются: повышение результативности решения задач обеспечения безопасности в интересах всего общества, поддержка реализации программ электронного правительства, развитие технических и человеческих ресурсов для гарантии устойчивого развития, использование технологий для улучшения поддержки служб принятия решений.

Согласно тексту документа, размещенному на портале ЮНИДИР, политика в указанной сфере включает следующие компоненты.

- Распространение коммуникационных и информационных услуг среди всех сообществ, улучшение и снижение их стоимости, модернизация инфраструктуры национальной сети и объединение баз данных для развития этих услуг.
- Подготовка кадров для ИКТ-отрасли, чтобы удовлетворить потребности сектора и сформировать поколение йеменской молодежи, способное справляться с требованиями эпохи цифровизации, а также создание новых рабочих мест.
- Развитие национальной индустрии разработки программного обеспечения и поощрение частного сектора к инвестированию в ИКТ и передовые технологии.
- Содействие повышению эффективности деятельности государственных органов, экономических и социальных секторов страны, создание ядра электронного правительства и электронной торговли, предоставление инфраструктуры и услуг для повышения качества науки и образования, здравоохранения и др.
- Организация взаимодействия государственного и ИКТ-секторов, регулирование их отношений и оценка обязательств.
- Защита информационно-коммуникационных сетей и сети Интернет от киберугроз.
- Содействие в разработке планов оптимальных инвестиций в целях сохранения суверенитета государства, обеспечения его безопасности и усиления защиты.

Для общественного обсуждения еще в октябре 2021 г. была представлена «Политика облачных вычислений», но результаты до сих пор не опубликованы.

В июле 2021 г. Йемен провел первую Национальную конференцию по кибербезопасности, целью которой стало обсуждение стратегии развития государ-

ственной политики в этой сфере. На конференции были рассмотрены три рабочих документа, посвященных оценке кибербезопасности в Йемене, требований проекта Национальной стратегии кибербезопасности, правовым и законодательным мерам противодействия киберпреступности, техническим мерам по защите информационной безопасности в национальной телекоммуникационной сети. Обсуждались 20 рабочих документов по информационной безопасности, киберпреступности, законодательству и правовым нормам, которые обеспечивают защиту пользователей в сетях связи, компьютерных и телекоммуникационных системах.

Правительству Йемена было рекомендовано автоматизировать работу всех министерств, чтобы облегчить доступ к информации и государственным данным. Премьер-министр на открытии конференции сказал: «Запад, возглавляемый Соединенными Штатами, старается изо всех сил, чтобы завладеть информацией и контролировать ее, в то время как Восток, возглавляемый Россией и Китаем, доказал свою способность конкурировать и создавать великую информационную революцию, что свидетельствует о продолжающемся обострении конфликта между крупными державами в этой области…» Он также подчеркнул, что непрекращающаяся агрессия против Йемена диктует необходимость принятия мер по укреплению информационной безопасности на постоянной основе.

3. Законодательство в сфере информационной безопасности

Национальное законодательство в сфере использования ИКТ и обеспечения информационной безопасности слабо развито и давно не актуализировалось.

Используется следующая нормативная база:

- Закон о телекоммуникациях 1991 года (с поправками от 1996 года);
- Декрет Республики Йемен №38 от 1991 года о развитии проводной и беспроводной связи;
- Закон о праве на доступ к информации 2012 года.

По состоянию на конец 2022 г. проект Закона о борьбе с электронными преступлениями находился в процессе разработки.

4. Основные угрозы информационной безопасности и общие подходы к противодействию этим угрозам, в том числе основные направления обеспечения информационной безопасности, включая используемые ключевые институты и инструменты защиты

К критически важной инфраструктуре Йемена относятся:

1. Сектор телекоммуникаций и информации: включает общественные телекоммуникационные сети, Интернет и компьютеры в домах, а также для академического, государственного и коммерческого использования.

2. Сектор физического распределения: включает автомобильные дороги, железные дороги, порты, водные пути, аэропорты, транспортные компании и грузовые службы, которые облегчают передвижение людей и товаров.
3. Энергетический сектор: отрасли промышленности, генерация и распределение электроэнергии, добыча и переработка нефти и газа.
4. Финансовый и банковский сектор: банки, другие компании, предоставляющие финансовые услуги, системы расчета заработной платы, инвестиционные компании, взаимные займы, ценные бумаги и физические обмены.
5. Сектор жизненно важных услуг: системы водоснабжения, службы экстренной помощи и государственные услуги.

Особое внимание уделяется следующим угрозам — фишинговые атаки, вредоносное программное обеспечение, атаки типа DDoS.

5. Государственные органы, входящие в систему обеспечения информационной безопасности

5.1. Национальный информационный центр (NIC)

Центр создан в середине 90-х годов с полномочиями реализации и формирования предложений по развитию государственной политики в сфере ИКТ, в том числе информационного контента. В 2000-х NIC разработал несколько проектов среди которых следует выделить Национальную информационную стратегию, создание Национальной информационной сети и Института информации, предложения в пятилетние планы социально-экономического развития Йемена. В соответствии с инициативами были созданы:

- Национальная комиссия высокого уровня для разработки отраслевых политик и стратегий;
- центры услуг для населения и публикации государственных данных;
- Йеменская электронная библиотека.

В настоящее время NIC является основным в системе обеспечения информационной безопасности Йемена. В его состав входит национальная группа реагирования на компьютерные чрезвычайные ситуации Yemen-CERT. Цель группы состоит в том, чтобы стать центром передового опыта в области информационной безопасности для Йемена, повысить уровень осведомленности и знаний об угрозах, для чего он сотрудничает с партнерами в целях координации усилий по предотвращению и устранению последствий компьютерных инцидентов. Однако для обращения к Yemen-CERT за помощью используется аккаунт в сети Facebook, что ставит под сомнение не только защищенность передаваемой информации, но и компетентность группы.

5.2. Министерство связи и информационных технологий (MTIT)

Министерство формирует политику по развитию телекоммуникаций и информационных технологий, которая является составной частью стратегии устойчивого развития страны. В 2005 году MTIT инициировало развитие национальной программы электронного правительства и при поддержке Экономической и социальной комиссия для Западной Азии ООН (ESCWA) разработало в 2011 году. Национальную стратегию e-Government. В настоящее время уровень зрелости электронного правительства оценивается как средний.

В 2022 году глава ведомства заявил, что деятельность Министерства направлена на создание безопасной и гибкой киберсреды в государственном и частном секторах, для чего его ведомство работает над завершением и обновлением соответствующей законодательной и правовой базы в области кибербезопасности, борьбы с преступлениями и защиты частной жизни путем принятия важных законов и законодательных актов, обновления и издания закона о борьбе с преступлениями в области информационных технологий и подготовки закона о защите персональных данных. Он указал на важность разработки политики для продвижения и поощрения цифровой инфраструктуры и национального цифрового контента, содействия созданию поставщиков цифрового контента и инвестиций в создание местных платформ передачи данных.

5.3. Министерство внутренних дел

В соответствии с инициативами национальной политики в сфере ИКТ создан профильный департамент «Информационный центр», функцией которого является применение информатизации для решения задач безопасности, продвижения информационной безопасности на ведомственном и государственном уровне, создания аналитической системы и органов поддержки принятия решений на долгосрочную перспективу. В Министерстве создано несколько информационных систем, обеспечивающих выполнение возложенных на него задач (оперативный сбор, анализ и своевременное распространение информации о текущей обстановке, обобщенный учет криминальной деятельности, предоставление геопространственных данных в военно-политических целях, в целях охраны границ и миграционных служб). По данным анализа, проведенного для Всемирного конгресса инженерных и компьютерных наук (2015), используемое Министерством аппаратное и программное обеспечение, базы данных и подготовка кадров не соответствуют современным требованиям.

6. Участие в международном сотрудничестве в области формирования системы обеспечения международной информационной безопасности в рамках ООН и позиция при голосовании по наиболее важным резолюциям ГА ООН

При голосовании по резолюциям резолюциям Генеральной Ассамблеи ООН о создании ГПЭ и РГОС Йемен всегда выступал в поддержку, а также стал соавтором резолюции Генеральной Ассамблеи ООН A/RES/70/237 от 23 декабря 2015 г., рекомендовавшей членам международного сообщества придерживаться норм ответственного поведения государств при использовании ИКТ.

7. Участие в международном сотрудничестве с другими международными организациями в области формирования системы обеспечения информационной безопасности на региональном уровне

Йемен является членом МСЭ и Организации исламского сотрудничества (OIC), в том числе ее платформы глобального сотрудничества по разработке политик и средств безопасности для смягчения киберугроз (OIC-CERT).

8. Содержание и оценка предложений и инициатив в области формирования системы обеспечения международной информационной безопасности

Предложения и инициативы Йемена в области международной информационной безопасности отсутствуют в связи с несформированной государственной политикой в этой сфере, слабостью нормативного обеспечения информационной безопасности и зачаточным состоянием системы защиты национального киберпространства.

8. КАТАР

Официальное название: Государство Катар
Столица: Доха
Официальный язык: арабский

Территория: 11 437 км² (158-я в мире). Катар расположен на восточном побережье Аравийского полуострова. Его территория состоит из ряда островов, в том числе Халул, Шраух, Аль-Асшат и другие. Граничит с Саудовской Аравией на юге, со всех остальных сторон омывается Персидским заливом. Площадь Катара составляет 11,521 км². Общая протяженность границы с Саудовской Аравией — 60 км.

Почти вся территория страны представляет собой пустыню. На севере — низкая песчаная равнина с редкими оазисами, покрытая движущимися (эоловыми) песками; в срединной части полуострова — каменистая пустыня с участками солончаков; на юге — высокие песчаные холмы.

Население: 2 753 045 чел. (по оценкам на 2019 год), что является 141-м показателем в мире.

Государственное устройство: Катар является абсолютной монархией. Система правления в Катаре основана на разделении и сотрудничестве властей. Исполнительная власть принадлежит эмиру и наследнику, которым помогает Совет министров, как это предусмотрено Конституцией, а законодательная власть принадлежит Консультативному совету.

Эмир является главой государства и представляет страну внутри страны, за ее пределами и во всех международных отношениях. Он также является главнокомандующим вооруженными силами, которыми он руководит при содействии Совета обороны, находящегося в его прямом подчинении. Судебная власть принадлежит судам общей юрисдикции, и судебные решения провозглашаются именем эмира.

Эмиру помогают Совет министров или кабинет, премьер-министр и шесть высших советов. Эмир назначает премьер-министра и министров, принимает их отставку и освобождает от занимаемых должностей указами эмира. Он поручает задачи каждого министерства министру или премьер-министру в соответствии с указом эмира о назначении.

Премьер-министр председательствует на заседаниях Совета министров и контролирует координацию работы между различными министерствами с це-

лью достижения единства и интеграции всех ветвей власти. Он также подписывает решения Совета.

Экономика: Показатели ВВП (Паритет покупательной способности) за 2021 год:

- Итого: $274,249 млрд (62-й показатель в мире)
- На душу населения: $104 740 (4-й показатель в мире)

Показатели ВВП (Номинал) за 2021 год:

- Итого: $179,677 млрд (55-й показатель в мире)
- На душу населения: $68 622 (5-й показатель в мире)

Дипломатические отношения с Россией (СССР): установлены 1 августа 1988 г.

1. Уровень развития системы обеспечения информационной безопасности и информационно-коммуникационной инфраструктуры

Диверсификация экономики за счет активной цифровизации и внедрения инноваций является стратегической целью Катара. Последние десять лет он входит в группу высокоинформатизированных стран. По данным МСЭ, эмират в 2017 году. занимал 39-е место в Глобальном индексе развития ИКТ.

Согласно результатам аналитических исследований ВЭФ в 2016 году уровень сетевой готовности Катара был поставлен на 27-ое место в мире. Государство обладает хорошо развитой и доступной ИКТ инфраструктурой, в Дохе в 2020 году. была открыта первая собственная точка обмена международным интернет-трафиком. Почти 94% домохозяйств обеспечены широкополосным доступом в Интернет. Более 70% жителей используют онлайн-банкинг. На одного катарца приходится 1,47 мобильных телефонных номера, в зоне покрытия мобильной связи 4G находится 99,5% населения, с 2018 года в густонаселенных зонах развертываются сети 5G.

По данным на 2017 год ИКТ-сектор Катара оценивался в $3,9 млрд, его вклад в ВВП составил 2,7%. По некоторым оценкам, в 2021 году национальный рынок программного обеспечения достиг $439,4 млн, сектор ИТ-услуг— $274,6 млн, ИКТ-инфраструктуры—$219,7 млн. Национальный рынок кибербезопасности ежегодно растет на 12,7% и в 2022 году должен был достичь $1,02 млн. Высоко развита электронная торговля, ее объем один из самых больших в регионе Ближнего Востока и Северной Африки. Государство и бизнес активно инвестируют в использование передовых ИКТ (искусственный интеллект, Большие данные, блокчейн), для этого созданы все необходимые регуляторные рамки.

Система электронного правительства Катара является одной из самых развитых, что подтверждается исследованием ООН «e-Government Survey 2018». Различным видам пользователей в 2019 году было доступно 2700 государственных сервисов и услуг, их объем с 2014 года возрос на 1721%. Кроме того, введены механизмы доступа к массивам Больших данных государственных ведомств для бизнеса и исследовательского сообщества, что стимулирует развитие приложений искусственного интеллекта.

Национальная политика в сфере информационной безопасности начала формироваться с 2009 года, во время кризиса отношений с партнерами по ССАГПЗ в 2014 году получила ускорение и в настоящее время является достаточно зрелой. Индекс ее развития очень высокий — в 2021 году страна заняла 27-е место в Глобальном рейтинге кибербезопасности МСЭ и 5-е место в регионе.

Однако общим слабым местом экономики Катара является недостаточное развитие национального кадрового потенциала[1]. В сфере кибербезопасности ощущается острый недостаток квалифицированных специалистов для обслуживания сложных информационных систем и инфраструктур в государственном секторе и бизнесе («умные города», аэропорты, ж/д). Это вынуждает к плотному техническому сотрудничеству с мировыми ИКТ-корпорациями и компаниями информационной безопасности, негосударственными организациями и НКО, а также к созданию большого количества частных фирм с международным участием. Образовательная система по модели STEM[2] в стадии становления, собственные НИОКР и стратапы только начинают развиваться, высокотехнологичный экспорт отсутствует.

2. Основные документы стратегического планирования в области обеспечения информационной безопасности

Основополагающим документом стратегии экономического, социального, человеческого и экологического развития Катара является программа «Видение 2030», принятая в 2009 году. В части ИКТ и информационной безопасности она дополняется следующими документами долгосрочного и среднесрочного планирования, которые учитывают перечисленные выше факторы экономического и технологического развития страны, а также быстрое изменение демографической ситуации — из 3 млн жителей Катара 17% составляет молодежь до 24 лет.

2.1. Вторая Национальная стратегия развития Катара (2018–2022 годы)

Задача полной цифровизации экономики и общества напрямую увязана с развитием национальной отрасли ИКТ. Одной из важнейших целей Стратегии является превращение Катара в региональный центр знаний и технического влияния. Огромное внимание уделяется повышению качества всех уровней образовательной системы[3], укреплению исследовательских центров, привлечению педагогического состава, развитию научно-технологического партнерства с ведущими арабскими и международными университетами. В стране учится боль-

1 В госсекторе 90% должностей занимают катарцы, в частном секторе 95% персонала — экспаты.

2 Образовательная модель STEM (Science, Technology, Engineering, Mathematics) объединяет в единую систему естественные науки и инженерию.

3 Уровень подготовки, особенно в инженерных дисциплинах и математике, в Катаре не соответствует мировым стандартам, что является серьезной проблемой. Результаты тестирования показывают, что 35% выпускников-математиков не смогли сдать экзамен (средний уровень по миру 7%) и только 3% достигли наивысших баллов (средний по миру 6%). В 2022 году поставлена задача на 50% увеличить выпуск специалистов по государственным программам подготовки инженеров и технологов, математиков, ученых.

шое количество иностранных студентов.

Для ускорения развития ИКТ-отрасли и трансфера технологий формируются новые механизмы поддержки бизнеса, в том числе через создание промышленных и инновационных технологических парков. Так, Цифровой инкубационный центр Катара предлагает новым стартапам возможность реализовать их идею и поддержать ее технологическое решение в течение шести месяцев, чтобы убедиться в его жизнеспособности. Для хорошо зарекомендовавших себя стартапов на два года предоставляются офисные помещения и наставничество по продвижению их продуктов. Особый потенциал роста у стартапов в сфере финансовых технологий (финтех). Например, молодая катарская компания QPAY реализовала с использованием технологии блокчейн крупнейшую в стране сеть финансовых услуг[4] для малого и среднего бизнеса, которая обслуживает 100 тыс. клиентов и 10 тыс. малых предприятий.

Государство является основным драйвером инноваций, активно развивая цифровизацию государственных органов и услуги электронного правительства, защищая критические информационные инфраструктуры (КИИ). Для обеспечения их устойчивости и надежности укрепляется «Щит электронной безопасности», включающий комплекс мер организационного, технического и правового характера.

В связи с этим Стратегией поставлены следующие задачи:

- обеспечение защиты информационных инфраструктур государственных органов (к 2022 году до 30 ведомств и организаций);
- расширение сети точек обмена международным трафиком и повышения ее эффективности;
- создание необходимой инфраструктуры для использования системы электронной подписи;
- борьба с киберпреступностью, расширение центра оперативного мониторинга электронной безопасности, создание лаборатории анализа цифровых доказательств, развитие центра информации об электронной безопасности;
- развитие и обновление системы сбора и анализа данных о цифровых угрозах в стране и мире, повышение потенциала по реагированию на компьютерные инциденты;
- подготовка квалифицированных национальных кадров по информационной безопасности (с 5 в 2016 году до 30 в 2022 году);
- укрепление международного сотрудничества, повышение количества выдвижений катарцев на посты в международных организациях и специали-

4 QPAY в партнерстве с NexxoNetwork (USA) создала децентрализованное приложение, позволяющее объединять локальные платежные инструменты на основе Ethereum Blockchain в глобальную систему.

зированных агентствах ООН (по 30 чел. ежегодно), использование дипломатических миссий для развития обменов на научном, коммерческом и образовательном уровнях в целях защиты национальных гигантов от новых угроз.

2.2. Стратегия развития электронного правительства (Qatar e-Government 2020)

Для разработки Стратегии и межведомственной координации деятельности по достижению ее целей в 2013 году был создан Наблюдательный комитет электронного правительства, в который вошли руководители 8 ключевых ведомств, включая министерство общих служб и финансов.

Создание единой системы электронного документооборота правительства и предоставления государственных услуг в цифровом виде стало объединяющим элементом движения Катара к формированию цифрового общества в соответствии с программой развития «Видение 2030», Национальной стратегей развития ИКТ (2015) и Национальным планом широкополосного доступа к Интернету (2016), Стратегией исследований, развития и инноваций (2018).

В период с 2013 по 2020 годы реализованы три этапа Стратегии развития, поставленные цели достигнуты. Создана защищенная сеть обмена данными, через которую все ведомства могут получить доступ к сервисами и услугам для взаимодействия между собой[5], объединенному государственному дата-центру[6], а также к службам электронного правительства и сети Интернет. Для этого введены политики доступа, защиты персональных данных и использования информации, а также стандарты взаимодействия. Эффективность работы ведомств оценивается с применением методов искусственного интеллекта на основе собираемой этой сетью бизнес-аналитики.

В настоящее время 100% государственных услуг можно получить в цифровом виде, в том числе осуществление государственных электронных платежей. Введена в действие уже третья версия веб-портала электронного правительства Hukoomi, которая обеспечивает доступ к 1400 онлайн сервисам для всех видов пользователей[7] и устройств доступа. С мобильного телефона через портал МВД Metrash доступны 174 услуги, в том числе получение лицензии на автомобили. Через портал Министерства торговли Al-Nadeeb можно осуществлять торговые и таможенные операции, по состоянию на январь 2022 г. их обработано более 3 млн.

Более 650 сервисов персонифицированы и используют криптографические

5 Например, электронному документообороту, службе обмена короткими сообщениями (sms), внутренней электронной почте.

6 В 2021 г. оператором дата-центра корпорацией Ooredoo начато развертывание новой версии оборудования с уровнем безопасности Tier III, что для обеспечения отказоустойчивости требует подключения двух независимых источников электроэнергии.

7 Бизнеса и государственных служащих, граждан и резидентов, путешественников.

методы для электронной подписи, цифровой идентификации, аутентификации с применением eID карт (выдаются гражданам Катара с 21 года и экспатам, содержат большой набор биометрических данных).

Использование единой цифровой среды обеспечивается государственной телекоммуникационной корпорацией Ooredoo на основе облачного сервиса (инфраструктура как услуга, IaaS).

2.3. Национальная стратегия кибербезопасности (2014)

Принятая в 2014 году Стратегия кибербезопасности была рассчитана на 5 лет. Она стала детализацией «Видения-2030» в части обеспечения национальной информационной безопасности за счет решения пяти основных задач:

- повышения защищенности КИИ (10 секторов, включая правительство, энергетику, финансы, телекоммуникации, транспорт и здравоохранение);
- улучшения системы предупреждения компьютерных инцидентов, выявления и реагирования на них, минимизации последствий и восстановления информационных систем за счет своевременного обмена информацией и координации действий;
- нормативно-правового обеспечения защиты киберпространства;
- повышения культуры кибербезопасности для безопасного и надлежащего использования ИКТ;
- развитие национального потенциала в сфере кибербезопасности.

Реализация Стратегии дала свои результаты, к настоящему моменту каркас системы защиты национального информационного пространства создан.

По оценке западных экспертов, недостатком этой системы является отсутствие четких показателей эффективности всех компонентов. Кроме того, ими отмечается отставание развития технической составляющей реагирования на киберугрозы, особенно в части наступательных средств. В связи с этим обращает на себя внимание перераспределение с 2016 года функционала между гражданскими и силовыми ведомствами и наделение последних широким кругом полномочий. Данные о разработке стратегии кибербезопасности на новый период в открытых источниках информации не выявлены, что также может свидетельствовать о смещении основных мероприятий киберзащиты в оборонную сферу.

3. Законодательство в сфере информационной безопасности

1. Закон о телекоммуникациях (Декрет № 34 от 2006 года) создал правовые рамки развития информационного общества. Он обеспечил развитие электронного правительства (в том числе политик развития систем и услуг, управления контентом, документооборота и регистрации, определения

ИКТ-архитектур и стандартов) и защиту киберпространства.

2. Закон об электронной торговле и сделках (№ 16 от 2010 года) — первый всеобъемлющий закон об электронных транзакциях и электронной торговле[8]. Он включает положения о таких областях, как электронные подписи, электронные документы и аутентификация; охватывает операции электронной коммерции и предоставление услуг электронного правительства. Не распространяется на документы, которые по закону должны быть нотариально заверены и оборотные документы, имеющие статус семейных и личных. Устанавливает наказания за компьютерные преступления, включая незаконный доступ к информационным системам, кражу личных данных, перехват информации или незаконное вмешательство в информационную систему.
3. Закон о предотвращении киберпреступности[9] (№ 14 от 2014 года). Регулирует преступления, связанные со взломом информационных систем, информационных программ, веб-сайтов. Закон определяет пять видов преступлений, ответственность за совершение которых в Катаре очень высокая:
   - Подделка официальных электронных документов (десять лет тюрьмы или штраф 200 тыс. катарских реалов), неофициальных документов — три года тюрьмы.
   - Мошенничество и кража данных (в основном касается неавторизованного доступа к электронным картам) — три года тюрьмы.
   - Утечки данных (кража интеллектуальной собственности, патентов, данных, относящихся к коммерческой тайне, и т.п.) — три года тюрьмы, штраф до 500 тыс. катарских реалов.
   - Фишинг — три года тюрьмы или штраф до 100 тыс. катарских реалов.
   - Распространение незаконного контента, в первую очередь детской порнографии и недостоверных данных, пять лет тюрьмы.

Катар также ратифицировал Арабскую Конвенцию о борьбе с преступлениями в области информационных технологий (2010), положения которой учтены в указанном Законе.

4. Закон о защите конфиденциальности персональных данных[10] (№ 3 от 2016 года, вступил в силу в январе 2017 г.).

Катар стал первой арабской страной Персидского залива, принявшей подобный закон. Его положения относятся только к персональным данным, которые обрабатываются в электронном виде или получаются, собираются или извлекаются для подготовки к электронной обработке, либо когда используется комбинация электронной и традиционной обработки.

Согласно закону организации должны соблюдать основные обязанности по

8 https://www.motc.gov.qa/sites/default/files/documents/e-Commerce_Law_EN.pdf
9 https://www.almeezan.qa/LawPage.aspx?id=6366&language=ar
10 https://almeezan.qa/LawPage.aspx?id=7121&language=ar

защите данных: обеспечение надлежащей подготовки операторов данных и принятие необходимых мер предосторожности для «защиты личных данных от потери, повреждения, изменения, раскрытия или несанкционированного доступа».

В соответствии со статьей 17 владелец или провайдер любого веб-сайта, связанного с детьми, должен установить политику в отношении того, как он обращается с информацией о несовершеннолетних. Провайдеры должны получить согласие родителей ребенка на обработку этой информации.

Закон о защите данных предусматривает высокие финансовые санкции за несоблюдение или нарушение законодательства, при этом отсутствуют наказания в виде лишения свободы.

Министерство транспорта и коммуникаций периодически выпускает руководства, дополняющие и разъясняющие особенности применения положений Закона. В 2019 году в связи со вступлением в силу Европейского Общего регламента обработки персональных данных их было 14, в том числе о сохранении записей об осуществленных действиях по обработке данных и оценке ее влияния на частную жизнь. В январе 2021 г. были выпущены руководства для частных пользователей, предприятий и руководителей, разъясняющие их обязанности и права, определенные Законом. В первую очередь, это касается уведомлений об утечках персональных данных, специальных форм запроса на их обработку, шаблонов и руководств по оценке воздействия на частную жизнь, особенностей применения некоторых статей.

4. Основные угрозы информационной безопасности и общие подходы к противодействию этим угрозам, в том числе основные направления обеспечения информационной безопасности, включая используемые ключевые институты и инструменты защиты

Киберпреступность в регионе Ближнего Востока и Северной Африки является вторым по распространению видом преступлений.

Наибольший резонанс получили следующие инциденты компьютерной безопасности в Катаре: заражение корпоративной сети газодобывающей компании RasGas вирусом Shamoon (2012), взлом регистратора доменных имен Катара силами Сирийской электронной армии (2013), кража из Национального банка 1,4 Гигабайт информации, в том числе в незашифрованном виде 15,5 тыс. внутрибанковских документов и данных клиентов (2016), взлом в период разрыва дипломатических отношений с соседними государствами ресурса Национального информационного агентства Катара с целью размещения тысяч фейковых постов о ситуации в стране (изначально связывали с деятельностью российских хакеров, после расследования американские специалисты связали инцидент с ОАЭ,

2017). В 2019 году массированная целевая фишинговая атака с использованием WhatsApp на национальную авиакомпанию QatarAirways. В период распространения пандемии Covid-19 использование недостаточно отработанного пользовательского приложения по отслеживанию социальных контактов привело к утечке персональных данных более миллиона человек. В 2021 году мощная четырехдневная DDoS-атака на международную телекомпанию Al Jazeera.

Основными угрозами информационной безопасности признаны использование вредоносного программного обеспечения, осуществление атак типа отказ в обслуживании (DDoS), электронное мошенничество, использование методов социальной инженерии для фишинга и других преступлений в сфере высоких технологий, распространение незаконного контента. Среди источников этих угроз названы хактивисты, преступные сообщества, террористические организации и инсайдеры.

Для противодействия этим угрозам применяются меры нормативного характера и организационно-технические меры.

В частности, с 2009 года реализуется Национальная политика гарантий информационной безопасности, обеспечивающая реализацию всеми участниками информационного взаимодействия единую научно-техническую политику в этой сфере. Политика основана на системе классификации значимости информации в бизнес-процессе предприятия, применении базовой трехуровневой системы безопасности и определении стандартных требований защиты информационной безопасности к каждому уровню (синтез методик ФРГ и Эстонии).

Указанная политика регулярно обновляется, в частности, в 2019 году к ней добавлены национальные стандарты безопасности: информации, облачных сервисов, систем промышленного контроля.

Центральный банк Катара, как регулятор, разработал для финансовой отрасли дополнительные требования по снижению рисков информационной безопасности, которые включают, но не исчерпываются следующими областями: управление технологическими рисками, дорожная карта обеспечения непрерывности бизнес-процессов, управление инцидентами и мошенническими случаями, детализированный контроль рисков.

В конце 2019 г. в Катаре впервые введены система аккредитации провайдеров, предоставляющих услуги в области информационной безопасности и система аккредитации безопасности программного обеспечения и гарантий безопасности для государственных электронных услуг. Это не только повысит безопасность ИКТ-продукции и услуг, но и уровень доверия к цифровой среде.

5. Государственные органы, входящие в систему обеспечения информационной безопасности

Министерство транспорта и информационных технологий (ictQATAR) переформатировано в 2016 году.[11] Оно является регулятором телекоммуникационной отрасли Катара и формирует технологическую политику и стандарты в сфере развития цифровых инноваций в различных сферах экономики и государства. С 2010 года оно обеспечивает функционирование электронного правительства и других информационных систем органов власти, обеспечивает безопасность национального киберпространства, лицензирование деятельности в сфере ИКТ.

Для выполнения этих функций три помощника замминистра ведут следующие направления:

- кибербезопасности (защита КИИ, защита персональных данных и соответствие стандартам, национальная группа реагирования на компьютерные инциденты Q-CERT);
- развития информационных технологий (управление государственными инфраструктурами, программы, стандарты и портал электронного правительства);
- развития цифрового общества (цифровизация производства и социальных сфер, наращивание кадрового потенциала цифрового общества, повышение осведомленности в сфере информационной безопасности).

В 2005 году в партнерстве с университетом Карнеги-Мелон (США) в структуре министерства создана Национальная группа реагирования на компьютерные инциденты Q-CERT, указанное сотрудничество сохраняется. Группа обладает развитым функционалом, поддерживает базу данных по лучшим практикам и стандартам информационной безопасности, устойчивости ИТ-систем и оценке рисков. Они доступны в качестве единого ориентира для государственных органов и других заинтересованных сторон.

Агентство регулирования коммуникаций, подведомственное ictQATAR, обеспечивает прозрачную и конкурентную среду в отрасли телекоммуникаций, распределяет радиочастотный спектр, выдает сертификаты соответствия техническим требованиям и стандартам ИКТ-продуктов и услуг, управляет пространством доменных имен, выдает лицензии операторам связи (в стране основными являются телекоммуникационные компании Ooredoo[12] и VodafoneQatar и опера-

11 С 2004 по 2013 год существовало в виде Высшего совета по информационно-коммуникационным технологиям, затем как Министерство коммуникаций и информационных технологий.

12 Ooredoo (ранее QatarTelecom) — крупный международный телекоммуникационный конгломерат с предприятиями в Ираке, Кувейте, Омане, Палестине, Индонезии, Лаосе, Мальдивах, Мьянме, Сингапуре, Алжире и Тунисе, обслуживающий 120 млн клиентов.

тор Национальной широкополосной сети — OBG).

Основными партнерами ictQATAR являются: по защите КИИ и реагированию — США; по развитию услуг электронного правительства осуществляется тесное взаимодействие с Эстонией; для укрупнения космической группировки спутников широкого спектра применения с 2010 года ведется сотрудничество с французской Eutelsat Communications. Взаимодействие с Израилем в сфере информационной безопасности осуществляется завуалированно, через субподряды европейских фирм или местные фирмы-однодневки (официальная политика поддержки Палестины не позволяет афишировать это взаимодействие).

Для развития государственно-частного партнерства в области защиты КИИ созданы Комитеты экспертов по информационным рискам (IREC) в финансовой сфере, энергетике, госсекторе и др. Они занимаются оценкой угроз, уязвимостями и последствиями их эксплуатации, выработкой стратегий повышения готовности и сокращения рисков. В целях повышения устойчивости сектора к кибератакам IREC обеспечивают защищенный обмен информацией с собственниками КИИ и другими заинтересованными сторонами.

С 2013 года Министерством проводятся ежегодные национальные учения кибербезопасности, которые включают отработку механизмов взаимодействия (командно-штабной тренинг) и практическое реагирование на инциденты. В СМИ есть упоминания об участии в них представителей зарубежных государств (Великобритании, Франции, США и Кувейта).

Министерство внутренних дел (MoI) в сфере информационной безопасности выполняет несколько функций. Прежде всего, это борьба с преступлениями в сфере высоких технологий, проведение расследований, обеспечение функционирования лаборатории цифровых доказательств.

Управление расследований Госбезопасности («Мабахис») занимается борьбой со шпионажем и связано с аналогичными структурами Израиля.

Кроме того, в состав Министерства из ictQATAR вошел национальный Центр кибербезопасности, который обеспечивает функционирование «электронного щита безопасности» страны[13]. Центр осуществляет защиту от кибератак почти 100 государственных органов и учреждений с государственным участием, направляет им уведомления об угрозах, средствах защиты и оказывает помощь в реагировании[14]. В нем функционирует служба мониторинга (Controlroom), в которую каждую секунду поступает до 35 тыс. сигналов об электронных инцидентах.

Еще одним фактом укрепления защитного потенциала страны является включение кибербезопасности в систему управления государством при чрезвычайных обстоятельствах. В 2016 году создан Национальный командный

13 англ. — Electronic Security Shield System (ESSE)

14 В открытых источниках факт перемещения в МВД Q-CERT не подтвержден.

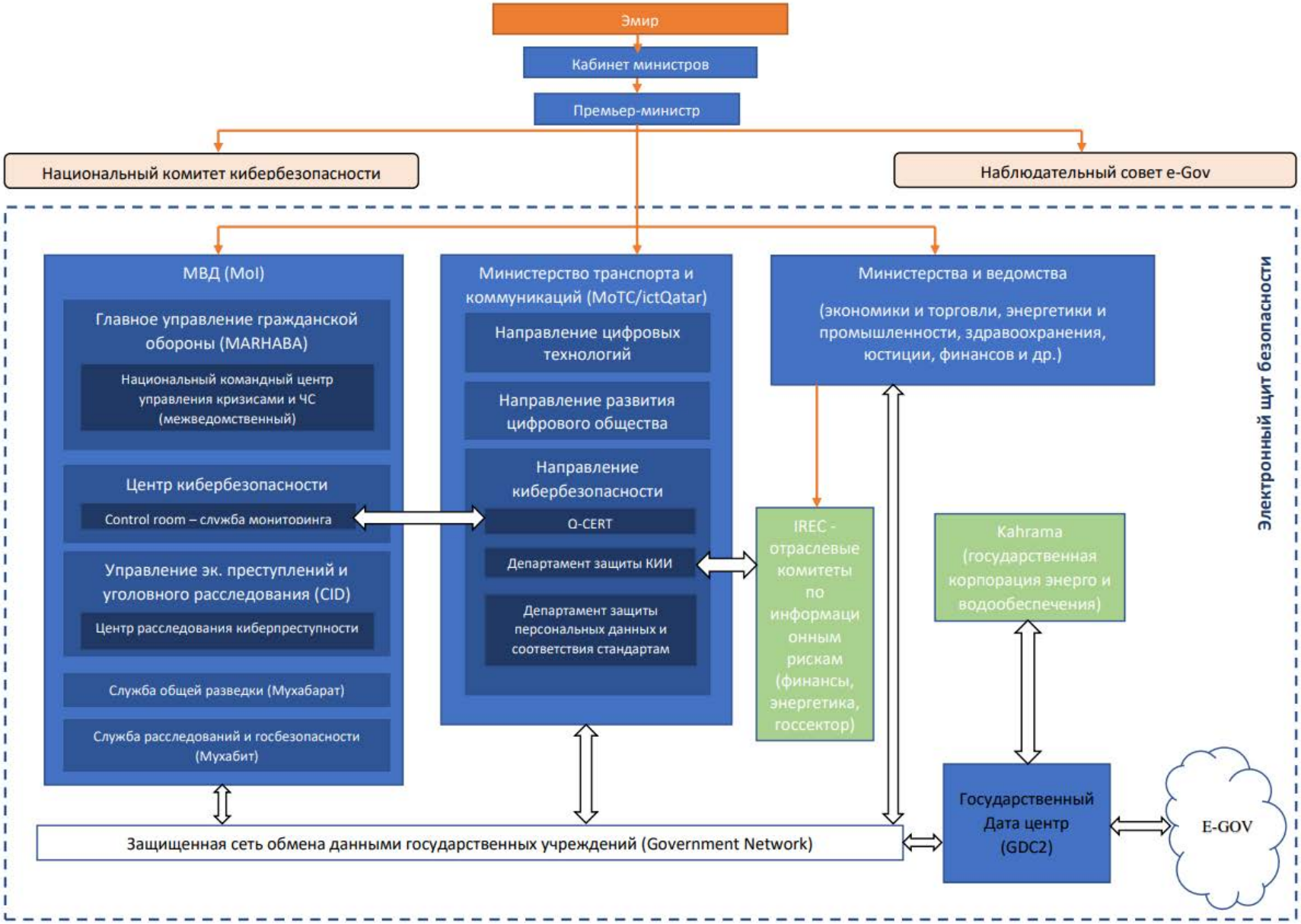


Рис. Организационная схема системы обеспечения информационной безопасности Катара

центр для управления кризисами в Главном управлении гражданской обороны (MARHABA) МВД Катара, который и продолжает его развитие. Центр в своем арсенале имеет «комнату управления электронной безопасностью», обеспечивающую связь с уполномоченными государственными органами для защиты КИИ от киберугроз и выработки политических решений, привлечения необходимых специалистов или проведения внешней экспертизы, взаимодействия с другими центрами реагирования и зарубежными партнерами.

6. Участие в международном сотрудничестве в области формирования системы обеспечения международной информационной безопасности в рамках ООН и позиция при голосовании по наиболее важным резолюциям ГА ООН

Представитель Катара был членом второго созыва ГПЭ в 2009–2010 годах и представил свои материалы к докладу ГПЭ, подчеркнув главенствующую роль ООН в решении рассматриваемых вопросов.

После созыва РГОС Катар принял участие в ее работе. Следует отметить, что Катар всегда поддерживал все резолюции по проблематике ГПЭ и РГОС, вместе с тем он не стал соавтором ни одной из них.

7. Участие в международном сотрудничестве с другими международными организациями в области формирования системы обеспечения информационной безопасности на региональном уровне

Катар является членом МСЭ и Организации исламского сотрудничества, присоединился к Парижскому призыву к доверию и безопасности в киберпространстве.

Программа кибербезопасности Катар-Турция[15] фокусируется на трех темах, связанных с проблемами кибербезопасности, которые разделяют обе страны: безопасность облачных вычислений и больших данных, системы безопасности для мобильных устройств и приложений, а также информационная безопасность критической инфраструктуры. Турецкая оборонная компания HAVELSAN и катарская Jaidah Group подписали соглашение о сотрудничестве, в рамках которого турецкие технологии будут использованы для повышения информационной безопасности ИКТ, энергетики и транспорта. На первом этапе HAVELSAN создаст в Катаре центр кибербезопасности и предоставит Jaidah Group доступ к своей платформе киберзащиты, потом Jaidah Group будет сотрудничать с местными университетами для «национализации» полученных технологий.

В 2014 году Великобритания и Катар заключили соглашения по борьбе

15 https://www.qf.org.qa/media-center/qnrf-tubitak-develop-new-cyber-security-program

с джихадом и киберугрозами. Штаб-квартира правительственной связи Королевства обязалась предоставить Катару продукты для обеспечения информационной безопасности и специальные средства ведения кибервойны.

Протоколом 2016 года о техническом сотрудничестве в киберпространстве и борьбе с киберпреступностью между МВД Республики Индии и МВД Государства Катар[16] установлено дополнительное техническое сотрудничество в указанной сфере к действующему рамочному соглашению в области безопасности от 10 ноября 2008 г.

В 2017 году Министерство транспорта и коммуникаций Катара подписало серию меморандумов о взаимопонимании с местными и международными игроками, включая Катарскую фондовую биржу (QatarStockExchange), Huawei и Пекинский международный исследовательский центр «Умный город», Эстонскую академию электронного правительства (Estonia's e-GovernmentAcademy) и американскую лабораторию пользовательского интерфейса UI Labs. Соглашения охватывают ряд проектов по разработке стартапов и предусматривают исследовательские проекты по следующим темам: открытые данные, Интернет вещей для «умных» городов, анализ Больших данных.

В 2018 году Председатель Государственной Думы Федерального Собрания Российской Федерации Вячеслав Володин и Председатель Консультативного совета Катара Ахмед Махмуд обсуждали возможность проведения конференции по кибербезопасности[17].

В 2021 году на Петербургском экономическом форуме пописана серия меморандумов о взаимопонимании, включая соглашение между Агентством по привлечению инвестиций Катара и российской компанией BI.ZONE, заключены партнерские соглашения с ведущими образовательными и культурными учреждениями Санкт-Петербурга и других регионов России, в том числе с ЛГУ и Санкт-Петербургским национальным исследовательским университетом информационных технологий, механики и оптики.

Для повышения эффективности своей работы Центр кибербезопасности МВД Катара заключил соглашение с Cisco International Company о сотрудничестве, а также о подготовке кадров для обеспечения информационной безопасности Чемпионата мира по футболу. К разработке и реализации плана мероприятий чемпионата мира по футболу Qatar 2022 Cybersecurity Framework были привлечены и другие американские корпорации — Microsoft, RSA, Dell, IBM, Hewlett Packard и компании информационной безопасности FireEye и SecureWork, а также катарское подразделение Университета Карнеги—Мел-

16 http://www.mea.gov.in/bilateral-documents.htm?dtl/27739/List+of+agreements+exchanged+during+the+visit+of+Prime+Minister+of+Qatar+to+India

17 https://dumatv.ru/news/rf-i-katar-dogovorilis-provesti-konferenciyu-po-kiberbezopasnosti

лона.

8. Содержание и оценка предложений и инициатив в области формирования международной информационной безопасности

В регионе Катар стремится к укреплению своего интеллектуального лидерства в сфере обеспечения информационной безопасности и повышению влияния «мягкой силы». В связи с этим он проводит целый комплекс крупных мероприятий и выставок по указанной проблематике, среди которых следует упомянуть ежегодный саммит для лидеров CYBERX QATAR SUMMIT и Конгресс по киберпреступности (e-Crime and Cybersecurity Congress Qatar).

В 2021 году Катар впервые провел Всемирный саммит по кибербезопасности, как ориентированную на бизнес инициативу по снижению актуальных угроз информационной безопасности. Мероприятие вызвало большой и позитивный резонанс. В июле 2022 г. саммит прошел в гибридном формате и был посвящен наиболее актуальным темам: искусственный интеллект для информационной безопасности, Интернет вещей и целостный подход к обеспечению безопасности киберфизических систем критических инфраструктур, управление идентификацией и доступом, применение технологий блокчейн, совместное использование Больших данных и интеллектуальное управление данными в системах массового обслуживания. Благодаря тематике интерес к мероприятию был очень высоким.

9. КОМОРЫ

Официальное название: Союз Коморских Островов

Столица: Морони

Официальные языки: коморский, французский и арабский

Территория: 2235 км² (168-я в мире). Государство расположено на вулканическом архипелаге Коморских островов, включающем четыре главных острова. Острова Нгазиджа (Гранд-Комор), Ндзуани (Анжуан) и Мвали (Мохели) фактически составляют Союз Коморских Островов, а остров Майотта фактически имеет статус «заморского региона» Франции, но на него претендует Союз Коморских Островов. Высшая точка — действующий вулкан Картала (2361 м). Острова гористы, окружены коралловыми рифами. Верхние части склонов гор покрыты густыми тропическими лесами, ниже располагаются саванны и кустарниковые заросли.

Население: 806 153 чел. (по оценкам на 2016 год), что является 164-м показателем в мире.

Государственное устройство: По форме правления Коморы являются федеративной президентской республикой. В соответствии с Конституцией 2001 года президент страны избирается на 4 года. До принятия на конституционном референдуме соответствующих изменений кандидатов представляли в порядке очередности каждый из трех островов.

Национальная ассамблея Союза Коморских Островов — законодательный (представительный) орган страны, состоящий из 33 депутатов. Из них 18 избираются всеобщим голосованием, 15 — ассамблеями трех островов на пятилетний срок.

Экономика: Показатели ВВП (Паритет покупательной способности) за 2019 год:

- Итого: $2,373 млрд (177-й показатель в мире)
- На душу населения: $2789 (161-й показатель в мире)

Показатели ВВП (Номинал) за 2019 год:

- Итого: $1,184 млрд (177-й показатель в мире)
- На душу населения: $1391 (168-й показатель в мире)

Дипломатические отношения с Россией (СССР): установлены 6 января 1976 г.

1. Уровень развития системы обеспечения информационной безопасности и информационно-коммуникационной инфраструктуры (включая индекс развития ИКТ по оценкам МСЭ и ООН)

По данным МСЭ за 2021 год, Коморы занимают в глобальном рейтинге кибербезопасности 175-е место и 20-е место в ЛАГ. Уровень проникновения Интернета в настоящее время составляет 21,8%. Индекс кибербезопасности составляет всего 3,72 из 100.

Исходя из перечисленных статистических данных, уровень развития системы информационной безопасности Коморов может быть оценен как очень низкий.

2. Основные документы стратегического планирования в области обеспечения информационной безопасности

Закон Союза Коморских островов от 29 декабря 2020 г. № 20-38/АУ закрепил в разделе I главы IV раздела V Уголовного кодекса (статьи 449–505) новые беспрецедентные меры для борьбы с киберпреступностью, которые регулирует четыре важных раздела:

- ✓ преступления, связанные с информационно-коммуникационными технологиями (доступ, поддержание, воспрепятствование нормальной работе информационной системы, мошенническое введение данных в информационную систему, мошеннический перехват данных, а также изменение данных и т.д.);
- ✓ нарушения прав интеллектуальной собственности в Интернете (посягательства на интеллектуальную собственность, совершаемые с помощью информационной системы, касающейся воспроизводства, предоставления общественности частично или полностью через информационную систему, произведения, защищенные авторским правом или смежным правом, и т.д.);
- ✓ незаконные действия в сетях электронной связи (организация незаконных онлайн-игр, ответственность физических лиц и других банковских учреждений за денежные переводы, связанные с незаконными онлайн- играми, и т.д.);
- ✓ ответственность технических поставщиков онлайн-услуг (доступ к интернет-услугам из интернет-кафе, условия доступа несовершеннолетнего в интернет-кафе и ответственность оператора, ответственность поставщиков услуг интернета и т.д.).

Также Закон регулирует поведение людей в социальных сетях, запрещение актов ксенофобского характера, оскорблений, распространения данных, которые

могут нарушить общественный порядок или могут нанести ущерб человеческому достоинству, разглашения ложной информации и т.д.

3. Основные угрозы информационной безопасности и общие подходы к противодействию этим угрозам, в том числе основные направления обеспечения информационной безопасности, включая используемые ключевые институты и инструменты защиты

Планируемые меры по укреплению кибербезопасности:

- ✓ совершенствование специального законодательства по кибербезопасности в рамках дематериализации и защиты киберпространства Союза Коморских Островов;
- ✓ совершенствование защиты персональных данных путем пересмотра закона 2014 года;
- ✓ дематериализация процесса тендерных заявок путем пересмотра кодекса государственных закупок;
- ✓ разработка закона об электронной коммерции.

Главная цель — создать к 2024 году расширенную правовую базу с помощью Цифрового кодекса.

Стратегия «Цифровые Коморы 2028»

Функции Стратегии:

- ✓ осуществление политики и программ, связанных с развитием использования цифровых технологий;
- ✓ обеспечение совместно с соответствующими органами власти и организациями внедрения и технического администрирования цифровых коммунальных услуг в рамках программы электронного правительства на основе их совместимой работы и безопасности;
- ✓ внедрение и обеспечение соблюдения в соответствующих органах власти и ведомствах стандартов и стандартов цифровых услуг и продуктов;
- ✓ создание совместно с соответствующими органами власти и учреждениями надлежащих механизмов кибербезопасности для обеспечения безопасности цифровых активов страны и сохранения суверенитета коморского киберпространства;
- ✓ консультирование и поддержка правительства в улучшении деловой среды в секторе цифровых технологий;
- ✓ сопровождение различных участников отрасли в целях развития и конкурентоспособности на Коморских островах, организация мероприятий по стимулированию инноваций и предпринимательства;
- ✓ обеспечение совместно с соответствующими учреждениями и органами

власти развития людских ресурсов, необходимых для реализации Национальной стратегии развития цифровых технологий;

- ✓ обеспечение конвергенции и согласованности различных государственных инициатив в области цифровых технологий;
- ✓ разработка программы партнерства и сотрудничества в области цифровых технологий с внешними предприятиями;
- ✓ предоставление государству информационной системы и вспомогательных инструментов для принятия решений;
- ✓ предоставление гражданам и предприятиям децентрализованного интерфейса доступа к администрации;
- ✓ оценка влияния инвестиций, реализуемых в IT-области.

Национальное агентство по развитию цифровых технологий (ANADEN) создано на основании Декрета NDEG 19-014 / PR от 10 января 2019 г. и предназначено для обеспечения разработки и реализации Национальной стратегии развития цифровых технологий.

Основные задачи Агентства:

- ✓ разработка Цифрового кодекса, который будет сопровождать, в частности, культуру, искусство и музыку, цифровое искусство;
- ✓ поддержка цифровизации, укрепление наследия и нематериального культурного наследия;
- ✓ сопровождение создания неправительственных организаций, занимающихся продвижением гендерной проблематики.

Развитие сферы кибербезопасности в рамках деятельности заинтересованных сторон:

Для цифрового сектора:

- Министерство почты и телекоммуникаций, отвечающее за цифровую экономику,
- Национальное агентство по развитию цифровых технологий (ANADEN),
- Национальный орган по регулированию информационно-коммуникационных технологий (ANRTIC),
- Коморская Ассоциация информационно-коммуникационных технологий (ACTIC).

Для сотрудников Службы безопасности:

- Министерство внутренних дел.

Для партнеров по развитию:

- Всемирный банк в рамках четвертого этапа региональной программы инфраструктуры связи.

4. Участие в международном сотрудничестве в области формирования системы обеспечения международной информационной безопасности в рамках ООН и позиция при голосовании по наиболее важным резолюциям ГА ООН

Коморы поддерживают российские инициативы в области международной информационной безопасности.

В 2018–2020 годах Коморы голосовали в поддержку российских проектов резолюций Генеральной Ассамблеи ООН:

A/RES/73/27 от 5 декабря 2018 г. (принятие правил, норм и принципов ответственного поведения, а также создание Рабочей группы ООН открытого состава);

A/RES/74/247 от 27 декабря 2019 г. (создание специального межправительственного комитета экспертов открытого состава для разработки всеобъемлющей международной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях).

В этот же период Коморы выступили соавтором российского проекта резолюции Генеральной Ассамблеи ООН A/RES/75/240 от 31 декабря 2020 г. (создание новой Рабочей группы ООН открытого состава по вопросам безопасности в сфере использования ИКТ и самих ИКТ 2021–2025).

При голосовании за принятие американского проекта резолюции Генеральной Ассамблеи ООН A/RES/73/266 от 22 декабря 2018 г. (о создании Группы правительственных экспертов ООН на 2019–2021 годы) Коморы проголосовали против.

5. Участие в международном сотрудничестве с другими международными организациями в области формирования системы обеспечения информационной безопасности на региональном уровне

Коморы взаимодействуют на глобальном и региональном уровнях по вопросам обеспечения кибербезопасности в рамках следующих международных организаций, членом которых они являются:

ООН;

ITU (МСЭ);

Движение неприсоединения;

Африканский союз;

ЛАГ;

Интерпол.

6. Содержание и оценка предложений и инициатив в области формирования системы обеспечения международной информационной безопасности

Коморы:

не стали соавтором инициативы Франции и Египта — Программа действий ООН по продвижению ответственного поведения государств в киберпространстве (2020 год);

не присоединились к инициативе Франции — Парижский призыв к доверию и безопасности в киберпространстве (2018 год).

10. КУВЕЙТ

Официальное название: Государство Кувейт

Столица: Эль-Кувейт

Официальные языки: арабский и английский

Территория: 17 820 км² (152-я в мире). Кувейт расположен на северо-востоке Аравийского полуострова и на островах Персидского залива — Бубиян, Файлака, Варба, Куббар, Кару, Умм-эль-Марадим и др.

Большая часть территории покрыта пустынями. Ландшафт равнинный, местами холмистый, наивысшая точка 290 м над уровнем моря на крайнем западе страны.

Население: 4 207 000 чел. (по оценкам на 2019 год), что является 126-м показателем в мире.

Государственное устройство: По конституции, принятой в 1962 году, Кувейт — конституционная монархия.

Глава государства — эмир. Эмир назначает главу правительства, имеет право распустить парламент, подписывать законопроекты, а также возвращать их на доработку в Меджлис. Эмир — верховный главнокомандующий вооруженными силами Кувейта, он назначает руководителей на ключевые посты в армии Кувейта, в том числе командующих всеми родами войск. Согласно конституции эмир пользуется юридической неприкосновенностью. Эмир назначает премьер-министра из членов правящей семьи. Премьер-министр в свою очередь назначает посты в правительстве. Все министры — члены Национальной ассамблеи и, как минимум, один министр — избранный. Ключевые министерства возглавляют члены правящей семьи.

Законодательная власть принадлежит эмиру и однопалатному Национальному собранию. 50 депутатов избираются в ходе всеобщих выборов на четырехлетний срок, еще 15 назначаются премьер-министром.

Экономика: Показатели ВВП (Паритет покупательной способности) за 2019 год:

- Итого: $218,605 млрд (65-й показатель в мире)
- На душу населения: $46 018 (26-й показатель в мире)

Показатели ВВП (Номинал) за 2019 год:

- Итого: $135,387 млрд (56-й показатель в мире)
- На душу населения: $28 500 (33-й показатель в мире)

Дипломатические отношения с Россией (СССР): установлены 11 марта 1963 г.

1. Уровень развития системы обеспечения информационной безопасности и информационно-коммуникационной инфраструктуры

Кувейт является одним из самых информатизированных государств в мире, уровень проникновения Интернета в стране достиг 98,3%. Высокоскоростными сетями подвижной связи покрыта вся территория страны, Кувейт первым в регионе внедрил технологию 5G и является одним из ведущих мировых рынков по ее использованию. Согласно данным национального Агентства по коммуникационным и информационным технологиям:

- 100% населения Кувейта обеспечено подключением к широкополосной сети связи 4G, а 97% населения к передовым сетям 5G;
- 99,3% домохозяйств через широкополосные оптоволоконные подключения используют цифровые платформы;
- 95,7% физических лиц ежедневно используют Интернет;
- 84,2% жителей имеют учетные записи в социальных сетях.

Результаты проведенного анализа статистических данных и отчетов компаний информационной безопасности показывают, что защищенность национального информационного пространства высокая. По данным МСЭ за 2021 год, интегральный индекс кибербезопасности Кувейта, рассчитанный с учетом развития правовой системы обеспечения информационной безопасности, применяемых технических и организационных мер, реализации программ наращивания потенциала и участия в международном сотрудничестве, составил 75,05 (из 100). Это ставит Кувейт на 65-ю позицию в мире и на 9-ю среди государств-членов ЛАГ.

2. Основные документы стратегического планирования в области обеспечения информационной безопасности

Для анализа политики Кувейта в области обеспечения информационной безопасности важно отметить, что Кувейт является ключевым региональным партнером США и Великобритании, сотрудничество с которыми в области обеспечения безопасности давнее и тесное[1]. Влияние указанных стран на стратегическое планирование Кувейта в разных сферах обеспечения безопасности значительно, хотя обычно остается в тени.

2.1. Национальный план развития «Видение 2035»

План «Видение 2035» родился на базе подготовленного в 2010 году бывшим премьер-министром Великобритании Т. Блэром исследовательского отчета с ана-

1 С США осуществляется сотрудничество в сфере безопасности границ, на море, кибербезопасности и контртерроризма.

лизом последствий для Кувейта глубокого экономического кризиса, вызванного падением мировых цен на углеводороды. Рекомендации отчета были взяты за основу плана диверсификации экономики «Видение 2035», реализация которого началась в середине 2010-х годов.

В соответствии с планом идет внедрение передовых технологий и цифровизация всех отраслей экономики, развитие инфраструктур мирового уровня, прежде всего «умных городов», «зеленой» энергетики и нефтехимии, транспорта. Это позволит Кувейту стать региональным лидером в финансах, торговле, туризме, здравоохранении. Огромные ресурсы вкладываются в развитие национального человеческого потенциала, высококачественное образование становится визитной карточкой страны. Реформирована политика в сфере исследований и инноваций. Реорганизуется система государственного управления, в том числе за счет расширения электронного правительства, которое, по оценке ЮНИДИР, находится на высоком уровне.

В реализации различных проектов плана «Видение 2035» участвуют многие ведущие ИКТ-корпорации. В частности, компания Huawei имеет инвестиционную лицензию на $1,7 млрд на развитие сектора ИКТ Кувейта. Кроме того, в рамках инициативы «Один пояс, один путь» Китай участвует в строительстве «умных городов» и крупных инфраструктурных проектах.

2.2. Национальная стратегия кибербезопасности 2017–2020 годов

Разработка Стратегии кибербезопасности[2] страны проведена при непосредственном участии экспертов США и Великобритании. Ключевой задачей Стратегии является выстраивание системы государственно-частного партнерства между правительственными агентствами, частным сектором и ведущими мировыми компаниями информационной безопасности[3]. Для ее реализации была разработана дорожная карта и выделен $1 млрд на 3 года.

Реализация Стратегии позволила обеспечить решение задач плана «Видение 2035» за счет снижения рисков цифровизации и безопасного использования киберпространства для достижения целей устойчивого развития страны. Основными стратегическими целями документа были заявлены:

1. Внедрение культуры кибербезопасности.

---

2 https://citra.gov.kw/sites/ar/LegalReferences/Cyber%20Security.pdf

3 В первую очередь речь идет об американских компаниях, входящих в ВПК США. Booz Allen Hamilton еще в 2012 году открыла в Кувейте свой офис для развития проектов в государственном и частном секторе. Lockheed Martin и Raytheon запустили программы развития для поддержки инициатив Кувейта в сфере кибербезопасности. Активно работают компании Microsoft (основной поставщик технологий облачных услуг и высокопроизводительных дата-центров), Cisco (сетевая инфраструктура), TrendMicro (продукты кибербезопасности). Великобритания выделила $2,4 млрд для программы Kuwait Security по обмену опытом между двумя правительствами. Шведская Ericsson предоставляет технологии для Интернета вещей и мобильной связи 5G.

2. Обеспечение и непрерывная поддержка безопасности национальных активов, включая критические информационные инфраструктуры, национальные данные, коммуникационные технологии и сети.
3. Содействие сотрудничеству, координации и обмену информацией между национальными и международными органами в области кибербезопасности.

Данные о разработке Стратегии кибербезопасности на новый период в открытом доступе отсутствуют.

2.3. Цифровая стратегия Центробанка Кувейта (2018)

В сентябре 2018 г. Центробанк Кувейта объявил о новой стратегии развития финансовых услуг, для чего будут развиваться аналитика Больших данных с использованием технологий искусственного интеллекта и блокчейн. Также в планах создание в сотрудничестве с банками и сервисами платежей национальной платежной системы (KNPS). Имеются планы разработки национальной цифровой валюты, для чего создаются необходимые технологии, но окончательного решения по этому вопросу нет.

3. Законодательство в сфере информационной безопасности

Кувейт подписал и ратифицировал Арабскую Конвенцию по борьбе с преступлениями в сфере информационных технологий. С целью имплементации ее положений в национальную нормативную базу в 2015 году принят Закон о борьбе с киберпреступностью[4], который криминализирует незаконный доступ к компьютерам и информационным системам или сетям с намерением получить конфиденциальные правительственные данные или информацию.

В 2014 году в целях развития цифровой экономики и защиты пользователей приняты Закон о защите конфиденциальных данных и Закон о проведении электронных транзакций, обеспечивающие легитимность использования цифровых документов, электронных подписей и платежей, а также обеспечение при этом требований информационной безопасности.

В сентябре 2021 г. Агентством по коммуникационным и информационным технологиям (CITRA) разработаны Регуляторные рамки использования облачных вычислений. Документ, посвященный общим нормам внедрения и использования в Кувейте сервисов облачных вычислений и дата-центров. В дополнение к нему подготовлен целый набор обязательных и рекомендованных политик и руководств, которые способствуют практическому применению общих рамок, в частности: политика классификации данных, рекомендации по обеспечению

4 https://www.moi.gov.kw/main/content/docs/cybercrime/ar/law-establishing-cyber-crime-dept.pdf

безопасности данных, кибербезопасности и контролю качества стандартов, правила для провайдеров облачных услуг и их обязательства, руководство для пользователей облачных сервисов, руководство по облачной миграции. Принятие указанных норм свидетельствует о превращении Кувейта в крупный центр обработки данных, и развитии вокруг него развитой экосистемы цифровых услуг для различных отраслей.

4. Основные угрозы информационной безопасности и общие подходы к противодействию этим угрозам, в том числе основные направления обеспечения информационной безопасности, включая используемые ключевые институты и инструменты защиты

Национальная стратегия кибербезопасности среди основных угроз информационной безопасности перечисляет следующие:

- заражение вредоносным программным обеспечением;
- атаки по типу «отказ в обслуживании» (DDOS);
- компьютерные атаки с целью кражи персональных данных или защищенных правами интеллектуальной собственности;
- рассылка спама по электронной почте с целью вымогательства, мошенничества, кражи личных данных, получения несанкционированного доступа к информационным системам;
- саботаж или манипулирование системами и данными.

В период пандемии COVID-19, как и в других странах, существенно возросли угрозы безопасности, вызванные дистанционной работой, в том числе применение злоумышленниками вирусов-шифровальщиков.

4.1. Агентство по коммуникационным и информационным технологиям (CITRA)

Агентство по коммуникационным и информационным технологиям (Communication and Information Technology Regulatory Authority, CITRA[5]) было создано в 2014 году в рамках реорганизации государственного управления. Оно является независимым от Министерства коммуникаций регулятором ИКТ-отрасли, обеспечивает надзор за сектором телекоммуникаций, выдает лицензии и распределяет радиочастотный спектр, осуществляет мониторинг и защиту интересов пользователей и поставщиков услуг, обеспечивает конкурентную среду.

Функцией CITRA является внедрение высоких международных стандартов в целях модернизации услуг электронного правительства и обеспечения их доступности для граждан и жителей, реализация Стратегии кибербезопасно-

5 https://citra.gov.kw/sites/ar/Pages/Home.aspx

сти Кувейта в части, касающейся функций агентства. Для этого в его структуре создан Национальный центр кибербезопасности (National Cyber Security Center of Kuwait, NCSC), решающий три стратегические задачи.

Первая задача: Повышение уровня кибербезопасности.

- Повышать национальную осведомленность в области кибербезопасности среди всех слоев общества путем выявления ожидаемых рисков, связанных с использованием киберпространства, одновременно поощряя использование решений для обеспечения безопасности и предотвращения рисков.
- Сотрудничать с Министерством образования и Министерством высшего образования, аффилированными лицами в разработке учебных программ по кибербезопасности.
- Сотрудничать с частным сектором, операторами связи и мобильной связи, а также Интернет-провайдерами для повышения кибербезопасности и обеспечения защиты транзакций с данными, повышая осведомленность о киберрисках.

Вторая задача: Обеспечение функционирования системы защиты киберпространства.

- Организовать работу и координировать деятельность Группы реагирования на компьютерные чрезвычайные ситуации (NCSC-KW), которая выполняет роль технической платформы для обмена информацией и повышения кибербезопасности государственных учреждений, принимает превентивные меры предупреждения компьютерных атак, поддерживает жизненно важные секторы в Государстве Кувейт, защищает их системы и обеспечивает поддержку реагирования на компьютерные инциденты.
- Создать и поддерживать Центр управления безопасностью (SOC) критически важных секторов Кувейта для обеспечения непрерывного мониторинга событий в области кибербезопасности и разработки надлежащих средств реагирования.
- Развивать национальный потенциал в различных областях кибербезопасности, таких как борьба с киберпреступностью, разработка безопасного ПО, сетевая безопасность, применение и мониторинг законов и политик, а также реагирование на чрезвычайные ситуации в области информационной безопасности.
- Разработать национальные стандарты и критерии для классификации технологий информационной безопасности.
- Разрабатывать и поддерживать национальные планы реагирования на инциденты и обеспечения непрерывности бизнеса для управления кризисами кибербезопасности.

- Развивать и продвигать средства защиты гражданских и военных сетей страны для ограничения возможностей компьютерных атак.
- Разрабатывать и поддерживать национальную политику кибербезопасности и средства контроля для национальных критически важных сетей, электронных услуг и важнейших систем ИКТ.
- Следить за соблюдением правил кибербезопасности и национальной политики.

Третья задача: Поддержка системы обмена информацией.

- Развивать национальное партнерство по обмену информацией в сфере кибербезопасности, включающее государственные учреждения, частный сектор и ведущие компании по кибербезопасности.
- Разработать координационный механизм обмена информацией между региональными и международными учреждениями и участвовать в программах кибербезопасности для борьбы с киберугрозами, а также облегчить доступ к надежной информации и обеспечить эффективное реагирование на все потоки.
- Разработать национальный механизм отчетности о киберугрозах, атаках и компьютерных преступлениях (совместно с МВД).

Агентство CITRA плотно сотрудничает с компанией Cisco[6] по реализации инициативы обеспечения удаленной работы государственных учреждений, порожденной в период пандемии COVID-19.

4.2. Центральное агентство по сетевым технологиям (CAIT)

Агентство (Central Agency for Information Technology, CAIT) создано в 2006 году как подведомственная организация Министерства коммуникаций и информационных технологий Кувейта. Отвечает за разработку и внедрение политики и технологий электронного правительства, в том числе обеспечивает функционирование Интернет-портала электронного правительства (e.gov.kw), его колл-центра, сети распространения официальной информации и новостей, онлайн-системы правовой информации и национальной нормативной базы в сфере ИКТ. Обеспечивает функционирование дата-центра, обслуживающего интересы государственных ведомств, и разработку планов восстановления в условиях чрезвычайных происшествий.

4.3. Управление по борьбе с киберпреступностью МВД Кувейта

Управление[7] получает все данные о нарушениях закона в киберсфере и проводит расследования для обеспечения их достоверности и серьезности информа-

6 https://citra.gov.kw/sites/en/Pages/cisco.aspx
7 https://www.moi.gov.kw/main/sections/cyber-crime

ции, а также для принятия в отношении нарушений необходимых правовых мер. В обязанности Управления входит:

- Развитие национального потенциала в борьбе с киберпреступностью в соответствии с международными стандартами.
- Разработка и актуализация в соответствии с технологическим развитием законодательства о киберпреступности и кибербезопасности.
- Разработка национального механизма отчетности о киберугрозах, атаках и компьютерных преступлениях.
- Развитие международных полицейских партнерских отношений для совместного расследования и пресечения компьютерных преступлений.

5. Участие в международном сотрудничестве в области формирования системы обеспечения международной информационной безопасности в рамках ООН и позиция при голосовании по наиболее важным резолюциям ГА ООН

На заседаниях Первого комитета ООН Кувейт всегда голосовал за резолюции Генеральной Ассамблеи ООН о созыве ГПЭ[8] и РГОС.

6. Участие в международном сотрудничестве с другими международными организациями в области формирования системы обеспечения информационной безопасности на региональном уровне

Кувейт является членом Организации исламского сотрудничества и МСЭ, но значимых инициатив в сфере кибербезопасности в этих организациях не выдвигал.

В 2004 году Кувейт стал первым государством Персидского залива, которое присоединилось к Стамбульской инициативе о сотрудничестве с НАТО, и подписал соглашение по информационной безопасности в целях облегчения обмена конфиденциальной информацией. Сотрудничество успешно развивается. В сентябре 2017 г. начал действовать региональный Центр НАТО в Кувейте.[9] Он провел «Неделю НАТО», посвященную сотрудничеству в политических и военных вопросах, в программе НАТО «Наука ради мира и безопасности», в том числе исследующей вопросы киберзащиты и безопасности критической инфраструктуры. Представители НАТО и Кувейта также провели встречи на уровне экспертов по кибербезопасности, направленные на обновление Индивидуальной программы партнерства и сотрудничества, согласованной между НАТО и Кувейтом в 2014 году.

8 Однако, Кувейт никогда не присоединялся к числу их соавторов.
9 https://www.nato.int/cps/ic/natohq/news_147010.htm

В декабре 2019 г. Кувейт в ходе 23-й Конференции министров связи ЛАГ поддержал Арабскую цифровую декларацию. При этом генеральный директор CITRA подчеркнул, что сектор ИКТ является ключевой частью экономики всех стран мира,[10] и призвал арабское объединение и региональный блок сыграть ключевую роль в защите интересов стран в условиях проблем, вызванных глобальной цифровой трансформацией. В декларации сделано заявление об общих принципах построения процветающего и устойчивого цифрового арабского сообщества на пяти принципах: экономика — наша цель, молодежь — наш двигатель, данные — наше топливо, инновации — наше вдохновение, а единство — наша сила.

В октябре 2019 г. Кувейт и Эстония подписали Меморандум о взаимопонимании по расширению сотрудничества в области цифровой трансформации, особенно в сфере передовых финансовых технологий, кибербезопасности и борьбы с компьютерной преступностью, наращивания потенциала, в том числе обучения персонала для развития сервисов электронного правительства и проведения совместных тренировок.

7. Содержание и оценка предложений и инициатив в области формирования системы обеспечения международной информационной безопасности

Основные усилия Кувейта в области формирования системы обеспечения МИБ направлены на повышение авторитета страны путем применения инструментов «мягкой силы». Осуществляется большое количество образовательных программ, конференций и конкурсов для талантливой молодежи, предназначенных как для граждан Кувейта, так и для других стран региона. Кроме того, в Кувейте проводится множество региональных конференций по кибербезопасности, предоставляющих возможность обсуждения актуальных киберугроз и технологий для их снижения.

В сотрудничестве с Trend Micro ежегодно проводятся киберучения National Cybersecurity CTF.

Ежегодно в Дохе CITRA в сотрудничестве с МСЭ проводит Региональный форум МСЭ по стандартизации, который проходит в увязке с Региональным форумом по Интернету вещей, «умным» городам и Большим данным.

В 2018 году в Султанате Оман CITRA провело «Региональную неделю кибербезопасности»[11] в сотрудничестве с Арабским региональным центром кибербезопасности МСЭ. Мероприятия недели включали 7-ю Региональную конфе-

10 https://citra.gov.kw/sites/en/Pages/NewsDetails.aspx?NewsID=71
11 https://citra.gov.kw/sites/en/Pages/CyberSecurityWeek.aspx

ренцию по кибербезопасности в рамках 6-го Регионального семинара по оценке кибербезопасности.

Совместными усилиями Делового совета США-Кувейт и CITRA при участии большого количества американских ИКТ-компаний проводится Конференция по обмену опытом в сфере предотвращения утечек данных и вопросам регулирования кибербезопасности.

В октябре 2022 г. прошла четвертая конференция «Образование и исследования в сфере кибербезопасности ERC2022», проводимая CITRA совместно с посольством Великобритании, британской сетью научных и исследовательских учреждений (Science & Innovation Network) и большим количеством вузов и научных организаций Кувейта.

11. ЛИВАН

Официальное название: Ливанская Республика

Столица: Бейрут

Официальные языки: арабский и французский

Территория: 10 452 км² (161-я в мире). Ливан расположен на Ближнем Востоке. На западе омывается Средиземным морем, береговая линия 225 км. На севере и востоке граничит с Сирией, на юге — с Израилем. Сирийско-ливанская граница имеет протяженность 375 км, ливано-израильская — 79 км. Небольшой отрезок границы Ливана с Голанскими высотами (Фермы Шебаа), присоединенными Израилем, является спорной территорией.

Население: 6 856 000 чел. (по оценкам на 2019 год), что является 108-м показателем в мире.

Государственное устройство: Согласно конституции Ливан является парламентской республикой. Существующая более полувека «ливанская модель» (конфессионализм) государственного устройства была создана в 1943 году в процессе обретения Ливаном независимости от Франции. Для того, чтобы обеспечить более-менее равный доступ к верховной власти для всех религиозных конфессий, был разработан следующий порядок: президентом страны должен быть христианин-маронит, премьер-министром — мусульманин-суннит, спикером парламента — мусульманин-шиит, а в правительстве должны быть поровну представлены христиане и мусульмане.

Законодательная власть представлена Ассамблеей представителей — парламентом Ливана, который состоит из 128 депутатов, избираемых прямым голосованием на четырехлетний срок. В Ассамблее заседают 64 мусульманина (27 суннитов, 27 шиитов, 8 друзов и 2 алавита) и 64 христианина (32 маронита, 20 армян Армянской апостольской церкви, 2 армяно-католика, 7 православных, 1 греко-католик (мелькит), 1 протестант, а также еще 1 по усмотрению). Парламент избирает президента, утверждает состав правительства, утверждает законы и бюджет республики.

Экономика: Показатели ВВП (Паритет покупательной способности) за 2022 год:

- Итого: $44 443 млрд (89-й показатель в мире)
- На душу населения: $9732 (85-й показатель в мире)

Показатели ВВП (Номинал) за 2022 год:

- Итого: $18,08 млрд (79-й показатель в мире)
- На душу населения: $4577 (74-й показатель в мире).

Дипломатические отношения с Россией (СССР): установлены 5 августа 1944 г.

1. Уровень развития системы обеспечения информационной безопасности и информационно-коммуникационной инфраструктуры (включая индекс развития ИКТ по оценкам МСЭ и ООН)

Исходя из перечисленных ниже статистических данных, уровень развития системы информационной безопасности Ливана может быть оценен как низкий:

МСЭ 2021, индекс кибербезопасности: 30,44 (из 100)

МСЭ 2021, позиция в рейтинге среди государств-членов ЛАГ: 13

МСЭ 2021, позиция в глобальном рейтинге: 109

МСЭ, уровень проникновения Интернет: 81,3%

NCSI, уровень цифрового развития: данные отсутствуют

NCSI, индекс готовности к киберугрозам и реагированию на них: 19,48

2. Основные документы стратегического планирования в области обеспечения информационной безопасности

В настоящее время в правовом регулировании деятельности в области обеспечения кибербезопасности существуют проблемы, в том числе:

1) отсутствует единая Национальная стратегия кибербезопасности (затруднено сотрудничество в области обеспечения кибербезопасности без четко определенных критериев, ключевых показателей эффективности и обмена информацией, а также без общей структуры на национальном уровне).

Национальная стратегия должна быть направлена:

- на обеспечение того, чтобы кибербезопасность стала юридически обязательной и подлежащей исполнению целью для инфраструктуры информационной системы Ливана в целом;
- на повышение возможностей киберзащиты страны от множества различных киберпреступлений и вредоносных кибератак и представление структуры централизованного органа, находящегося в ведении Президиума Совета Министров, который будет отвечать за реализацию составляющих этой стратегии;

2) отсутствуют законы и нормативные акты, регулирующие борьбу с киберпреступностью (отсутствуют законы и нормативные акты, регулирующие защиту от киберугроз государственных учреждений, частных компаний, а также киберправа отдельных лиц; отсутствует законодательство в области противодействия использования ИКТ в преступных целях).

На государственном уровне ведется разработка Стратегии цифровой трансформации.

В рассматриваемой области имеется Закон № 81 от 2018 года «Об электронных транзакциях» — содержит главу о сохранении электронных доказательств.

3. Основные угрозы информационной безопасности и общие подходы к противодействию этим угрозам, в том числе основные направления обеспечения информационной безопасности, включая используемые ключевые институты и инструменты защиты

Основные угрозы кибербезопасности:

- ✓ киберзависимые преступления (когда устройства ИКТ могут быть как основным инструментом для совершения преступления, так и основной целью самого преступления: разработка и распространение вредоносных программ с целью получения финансовой выгоды; взлом с целью кражи конфиденциальных данных; DDoS-атаки; программы-вымогатели и шантаж; повреждение, изменение или уничтожение данных);
- ✓ киберпреступность (кибермошенничество, кража данных, шпионаж, грабежи, вымогательство, пропаганда или уничтожение в целях получения денег или данных для использования в других вредоносных действиях);
- ✓ кибершпионаж со стороны государств или организаций, спонсируемых государствами (попытки проникновения в киберпространство, общедоступную или частную сеть, а также в конфиденциальные файлы в облачных сетях для получения политического, дипломатического, военного, технологического, коммерческого, финансового и стратегического преимущества. Нацелены на важнейшие национальные инфраструктуры страны, такие как оборона, финансы, энергетика, здравоохранение, коммунальные услуги и телекоммуникационные активы);
- ✓ в террористических целях (использование Интернета в целях придания публичности, рекламы и пропаганды террористических организаций, вербовки и мобилизации, сбора средств, использования безопасной сети для обмена информацией, планирования и координации, взятия на себя ответственности за нападения, демонстрации своих возможностей в качестве метода запугивания):
- ✓ хактивизм (когда действия в основном преследуют разрушительную и преступную цель для своих жертв, использование Интернета в тех же целях, что и террористические организации);
- ✓ инсайдерские угрозы (совершаются злонамеренными инсайдерами, которые неявно являются «доверенными» сотрудниками организации и могут иметь доступ к критически важным системам и данным, в целях нанесения финансового и репутационного ущерба в результате кражи конфиденциальных данных и интеллектуальной собственности, а также в целях доступа для облегчения или запуска атаки с целью нарушения работы критически важных служб в сети своей организации или удаления данных из сети):

- ✓ детские сценарии (когда неопытные акторы используют для проведения кибератак сценарии или инструменты, разработанные другими пользователями и / или загруженные из Интернета):
- ✓ атаки компьютерной сети (при которых враждебные субъекты могут использовать вредоносное программное обеспечение для нарушения и повреждения киберинфраструктуры — от перевода веб-сайта в автономный режим до управления системами управления промышленными процессами).

Проблемы в области обеспечения кибербезопасности на национальном уровне:

1) отсутствие Национального агентства кибербезопасности, на которое могли быть возложены следующие функции:

- ✓ разработка и обеспечение соблюдение законов о кибербезопасности;
- ✓ привлечение специалистов с необходимым уровнем знаний для оказания помощи организациям в создании их систем безопасности;
- ✓ проведение тренингов;
- ✓ поддержание исследований и разработок;
- ✓ гарантирование непрерывности программ повышения осведомленности о кибербезопасности;

2) борьба между коррупцией и цифровой экономикой (коррупция и цифровая экономика диаметрально противоположны, поскольку коррупция является основной угрозой для внедрения кибербезопасности, в то время как цифровая экономика потенциально может уничтожить или нарушить коррупционные схемы);

3) многогранный социально-демографический контекст (государство должно обеспечить, чтобы люди, назначенные для реализации Стратегии кибербезопасности, были компетентными, надежными, опытными, ответственными за отстаивание общих интересов и продвижение общего блага, а также мотивированными сильным чувством патриотизма);

4) отсутствие сотрудничества между различными администрациями на национальном уровне (каждое учреждение работает над своей безопасностью отдельно без четких рамок сотрудничества с другими учреждениями, без обмена информацией; наблюдается недостаточное взаимодействие внутри учреждений для обеспечения их безопасности);

5) отсутствие активного участия частного сектора в продвижении государственного сектора (частный сектор не в состоянии успешно управлять передачей этих IT-проектов государственному сектору, и он не получил должной выгоды от завершения таких проектов);

6) отсутствие инициативы по Национальной информационной системе и Стратегии цифровой трансформации (существует очевидный и серьезный дисбаланс между учреждениями, а координация ИКТ не институционализирована на национальном уровне, что очень затрудняет обнаружение, идентификацию и управление инцидентами, связанными с кибербезопасностью. В такой среде эффективное использование кибербезопасности для защиты граждан, а также государственных или частных организаций, подвергающихся кибератакам, становится серьезно скомпрометированным).

Государственные органы, решающие задачи в области обеспечения кибербезпасности:

- Национальная комиссия учреждена в 2010 году премьер-министром Ливана в составе представителей основных правительственных учреждений и органов безопасности для разработки Национальной стратегии кибербезопасности и борьбы с киберпреступлениями.
- Бюро по борьбе с киберпреступностью создано в 2006 году Судебной полицией Сил внутренней безопасности для расследования жалоб, нарушений кибербезопасности и преступлений, связанных с технологиями, под надзором судебных органов, а также для обеспечения базовой осведомленности общественности и образовательных учреждений о последних киберугрозах и кибератаках.
- Министерство телекоммуникаций играет важную роль в развертывании достаточно эффективной инфраструктуры в интенсивном сотрудничестве с частными операторами и ливанским оператором связи OGERO и регулярно решает вопросы кибербезопасности с национальными заинтересованными сторонами, а также наладило координацию усилий с МСЭ электросвязи по улучшению индекса кибербезопасности в Ливане.
- Центральный банк (BDL) разработал и внедрил зрелую, основанную на стандартах, передовую и инновационную Программу кибербезопасности, которая позволяет BDL предвидеть и отражать кибератаки. Эта программа состоит из двух основных компонентов и постоянно соответствует новейшим мировым передовым практикам и стандартам в области ИТ-безопасности.
- Службы безопасности и разведки для расследований в целях предотвращения угроз национальной безопасности, включая кибератаки и кибершпионаж.

4. Участие в международном сотрудничестве в области формирования системы обеспечения международной информационной безопасности в рамках ООН и позиция при голосовании по наиболее важным резолюциям ГА ООН

Ливан поддерживает российские инициативы в области международной информационной безопасности, всегда голосуя за их принятие.

В 2018–2020 годах проголосовал в поддержку российских проектов резолюций Генеральной Ассамблеи ООН:

A/RES/73/27 от 5 декабря 2018 г. (принятие правил, норм и принципов ответственного поведения, а также создание Рабочей группы ООН открытого состава);

A/RES/73/187 от 17 декабря 2018 г. (включение в повестку дня ООН обсуждения вопроса о противодействии использованию ИКТ в преступных целях);

A/RES/74/247 от 27 декабря 2019 г. (создание специального межправительственного комитета экспертов открытого состава для разработки всеобъемлющей международной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях);

A/RES/75/240 от 31 декабря 2020 г. (создание новой Рабочей группы ООН открытого состава по вопросам безопасности в сфере использования ИКТ и самих ИКТ 2021–2025).

Проголосовал за принятие американского проекта резолюции Генеральной Ассамблеи ООН A/RES/73/266 от 22 декабря 2018 г. (о создании Группы правительственных экспертов ООН на 2019–2021 годы).

5. Участие в международном сотрудничестве с другими международными организациями в области формирования системы обеспечения информационной безопасности на региональном уровне

Ливан взаимодействует на глобальном и региональном уровнях по вопросам обеспечения кибербезопасности в рамках следующих международных организаций, членом которых он является:

ООН;

ITU (МСЭ);

Движение неприсоединения;

ЛАГ;

Интерпол;

ISO (Международная организация по стандартизации).

Основные направления развития международного сотрудничества в области кибербезопасности:

- ✓ взаимодействие с международными партнерами, такими как Интерпол, организации ООН (МСЭ, УНП ООН, ЮНИКРИ и т.д.), Представительство Европы в Ливане и европейские институты и агентства (Совет Европы, Европол, CEPOL, ENISA и т.д.), органы стандартизации (NIST, EBIOS и т.д.), а также международные и региональные группы реагирования на на чрезвычайные ситуации (CERT/CSIRTs);
- ✓ использование существующих сетей и отношений с ключевыми международными партнерами правительства и налаживание новых связей с другими международными организациями для обмена информацией о текущих и возникающих угрозах, а также для приобретения необходимого опыта;
- ✓ установление стратегических двусторонних отношений и открытие каналов диалога с ключевыми заинтересованными сторонами для обмена информацией о потенциальных инцидентах;
- ✓ налаживание международных партнерских отношений в борьбе с киберпреступностью путем привлечения преступников в зарубежных юрисдикциях к ответственности;
- ✓ сотрудничество с международным сообществом по вопросам киберпространства для согласования и повышения эффективности общего свода законов и нормативных актов в целях оптимизации сроков, процедур и затрат, создания или адаптации к общим механизмам управления кризисами, коммуникации и деэскалации.

6. Содержание и оценка предложений и инициатив в области формирования системы обеспечения международной информационной безопасности

Ливан:

присоединился к инициативе Франции — Парижский призыв к доверию и безопасности в киберпространстве (2018 год);

не стал соавтором инициативы Франции и Египта — Программа действий ООН по продвижению ответственного поведения государств в киберпространстве (2020 год).

12. ЛИВИЯ


Официальное название: Государство Ливия

Столица: Триполи

Официальный язык: арабский

Территория: 1 759 540 км² (16-я в мире). Общая протяженность сухопутной границы — 4 383 км, в том числе с Алжиром — 982 км, Чадом — 1 055 км, Египтом — 1 150 км, Нигером — 354 км, Суданом — 383 км, Тунисом — 459 км. Береговая линия страны (побережье Средиземного моря) — 1 770 км.

Население: 6 777 000 чел. (по оценкам на 2019 год), что является 109-м показателем в мире.

Государственное устройство: Фактически Ливия в настоящее время представляет собой конгломерат из нескольких квазигосударств. Каждый из регионов Ливии обладает собственной спецификой; уровень жизни, безопасность, развитие инфраструктуры в них очень разные.

В августе 2014 г. Всеобщий национальный конгресс был сменен всенародно избранным парламентом — Палатой представителей Ливии. 12 августа 2014 г. члены Палаты представителей проголосовали за избрание президента Ливии путем прямых выборов, приняли решение о немедленной ликвидации всех вооруженных формирований бывших повстанцев.

В декабре 2015 г. при поддержке Совета безопасности ООН было образовано Правительство национального согласия или единства (ПНС) и Президентский совет. Заседания кабинета проходят в Триполи. ПНС является международно признанным, легитимным правительством Ливии. Палата представителей поначалу поддерживала новое правительство, но впоследствии отозвала это решение, вступив в конфронтацию с ПНС. На востоке заседает альтернативное правительство, подчиняющееся Палате. Также Палата представителей поддерживает главнокомандующего Ливийской национальной армией.

Экономика: Показатели ВВП (Паритет покупательной способности) за 2017 год:

- Итого: $69,056 млрд (95-й показатель в мире)
- На душу населения: $10 709 (89-й показатель в мире)

Показатели ВВП (Номинал) за 2017 год:

- Итого: $30,211 млрд (85-й показатель в мире)

- На душу населения: $4685 (88-й показатель в мире)

Дипломатические отношения с Россией (СССР): установлены 4 сентября 1955 г.

1. Уровень развития информационно-коммуникационной инфраструктуры и системы обеспечения информационной безопасности

По данным МСЭ, до 2011 года Ливия располагала лучшей инфраструктурой электросвязи среди арабских государств, но за прошедшее с тех пор время политическая и социальная нестабильность нанесла ущерб и привела к разрушению сектора электросвязи. Несмотря на это, страна остается высокоинформатизированной, уровень проникновения Интернета в настоящее время составляет 84,2%. Однако интегральный индекс кибербезопасности Ливии, рассчитанный МСЭ с учетом развития правовой системы обеспечения информационной безопасности, технических и организационных мер, реализации программ наращивания потенциала и участия в международном сотрудничестве, в 2021 году составил всего 28,78 (из 100). Это существенно ниже общемирового показателя, в связи с чем в глобальном рейтинге Ливия занимает 113-ю позицию и 14-ю — в ЛАГ.

Уровень развития электронного правительства в Ливии ниже общемирового. Вместе с тем процесс идет и часть государственных услуг переводится в онлайн-формат, в частности, регистрация актов гражданского состояния, налоговые платежи и обработка персональных данных государственных органов.

2. Основные документы стратегического планирования в области обеспечения информационной безопасности

Система государственного планирования в рассматриваемой области практически не развита. В настоящее время Ливия находится в процессе разработки национальной стратегии кибербезопасности, ее задачи и цели уже намечены в Стратегическом плане для телекоммуникационного сектора. Государственными органами, ответственными за исполнение стратегии, определены Национальное управление информационной безопасности и охраны (NISSA) и Министерство информации.

2.1. Стратегический план для телекоммуникационного сектора[1]

План включает 7 задач, а также список инициатив для их решения. Целью является полная цифровизация всех секторов экономики для достижения быстрого и устойчивого социально-экономического развития государства.

Задача 1. Достижение доступных и недорогих коммуникаций для всех, а также содействие развертыванию инфраструктуры ИКТ для поддержки безопасных подключений граждан, бизнеса и правительств.

1 https://www.cim.gov.ly/web/image/946?unique=59569f86d28bdefcda07301024a1b954faf0ef63

Инициативы для решения задачи:

а) повышение осведомленности о преимуществах ИКТ, а также поддержка программ образования в этой области;

б) поощрение партнерства между государственным и частным секторами в распространении ИКТ-сетей;

в) отмена/ снижение тарифов или других налогов на оборудование ИКТ для малообеспеченных сообществ и секторов государственных услуг, таких как здравоохранение, образование и управление чрезвычайными ситуациями.

Задача 2. Обеспечить, чтобы политика, правила и нормы, установленные для сектора ИКТ, способствовали прозрачности регулирования, защите потребителя, развитию конкуренции и поддержке технологической нейтральности.

Инициативы для решения задачи:

а) пересмотреть и обновить/разработать нормативную базу, регулирующую ИКТ-сектор, чтобы обеспечить ее пригодность для решения поставленной задачи, а также учесть имеющийся международный опыт;

б) принять соответствующие законы, политику и практику для обеспечения справедливого доступа к инфраструктуре, услугам и обучению в области ИКТ.

Задача 3. Эффективное использование ИКТ для успешного управления и развития системы и процесса электронного правительства.

Инициативы:

а) разработать стратегию электронного правительства для улучшения работы правительства и поддерживать государственные услуги посредством использования ИКТ;

б) поддержание государственных услуг для граждан путем инновационного использования информационных справочных служб и правительственного портала;

в) использование ИКТ для облегчения обмена данными и информацией между государственными министерствами и поставщиками государственных услуг.

Задача 4. Обеспечить безопасность инфраструктуры ИКТ, включая целостность, конфиденциальность и доступность всех используемых систем данных.

Инициативы:

а) интеграция ИКТ в национальную стратегию реагирования на стихийные бедствия;

б) разработка политики кибербезопасности;

в) создание подразделения по расследованию компьютерных преступлений для обеспечения соблюдения закона в сфере кибербезопасности.

Задача 5. Улучшение экономического роста и устойчивого развития с помощью ИКТ.

Инициативы для решения данной задачи не конкретизированы.

Задача 6. Продвижение цифровой грамотности и развитие навыков для повышения производительности и разработки инноваций.

Инициативы:

а) обеспечение школ и университетов компьютерами и недорогим и устойчивым доступом к сети Интернет;

б) поддержка программ электронного обучения «обучение в течение всей жизни» для молодежи и взрослых с целью развития и обновления навыков;

в) координация местных и региональных возможностей обучения государственных лиц, принимающих решения, и сотрудников директивных органов политике в области ИКТ.

Задача 7. Подготовка Ливии к превращению в центр ИКТ в Африке.

Для реализации данной задачи предлагается создать нормативно-правовую базу, которая будет регулировать выдачу новых лицензий для размещения на территории страны международных точек обмена трафиком, а также развитие новых оптоволоконных соединений с соседними странами.

Ожидаемыми результатами Стратегического плана являются:

а) совершенствование управления для достижения интегрированных цифровых услуг;

б) развитие человеческих ресурсов, необходимых для развития и поддержания общества знаний;

в) поддержка экономической деятельности страны с помощью усовершенствованной коммуникационной инфраструктуры;

г) интеграция ИКТ в повседневную жизнь ливийцев;

д) удовлетворение национальных потребностей и приоритетов.

2.2. Закон о борьбе с киберпреступностью (2021)

Закон был ратифицирован Палатой Представителей Ливии на пленарном заседании 26 октября 2021 г. в ускоренном режиме, через день после включения в повестку дня парламента и без консультаций с экспертным сообществом[2]. Закон содержит множество неоднозначных формулировок, которые могут ограничивать свободу слова в стране. В частности, статья 4 гласит, что использование интернета и новых технологий считается «правомерным» при условии соблюдения «общественного порядка и морали». Следовательно, любое использование, нарушающее эти широко трактуемые понятия, может считаться незаконным.

2 Проект закона была опубликован в социальных сетях https://www.facebook.com/groups/247181823107369/posts/616824622809752

Статья 7 Закона о борьбе с киберпреступностью разрешает ливийским властям отслеживать все, что публикуется в социальных сетях «и на любых других технических платформах», а также позволяет Национальному управлению информационной безопасности и охраны (NISSA), административно-техническому правительственному органу Ливии, блокировать веб-сайты и контент без судебного приказа, если они «подстрекают к расовой или религиозной розни или экстремистским религиозным убеждениям, которые подрывают безопасность и стабильность общества или наносят ущерб его социальному миру». NISSA также может подвергать цензуре и блокировать доступ ко всем веб-сайтам и страницам, содержащим материалы, «противоречащие общественной морали», согласно статье 8 Закона.

Статья 9 регулирует использование средств шифрования, которые не могут быть экспортированы или импортированы «без лицензии и разрешения Национального управления информационной безопасности и охраны».

Статья 21 направлена против использования дипфейков и предусматривает наказание тюремным сроком не менее одного года за «комбинирование или смешивание чьей-либо фотографии или голоса без их письменного или электронного согласия с использованием Интернета или любых других цифровых средств с намерением причинить вред другим».

В статье 37 говорится о тюремном заключении на срок не менее пяти лет и штрафе для тех, «кто распространяет слухи или публикует информацию или данные, угрожающие безопасности или общественной безопасности в Ливии или любой другой стране».

Следует отметить, что Ливия не присоединилась к сотрудничеству в рамках Конвенции о борьбе с преступлениями в области информационных технологий ЛАГ (2010), Конвенции Африканского союза о кибербезопасности и защите персональных данных (2014), Будапештской конвенции Совета Европы (2001).

3. Национальная система обеспечения информационной безопасности

3.1. Национальное управление информационной безопасности и охраны (NISSA)

Управление[3] создано в 2013 году Постановлением Совета министров № (28)[4]. Одним из подразделений NISSA является Ливийская группа реагирования на компьютерные инциденты (Libya-Cert), главной задачей которой является защита государственных информационных систем и ресурсов. Цели NISSA:

3 https://nissa.gov.ly/
4 https://www.cim.gov.ly/authority-decision

а) координация между всеми государственными учреждениями для управления центром безопасности, чтобы обеспечить безопасную среду для обмена информацией и сообщениями;
б) подготовка законодательной и правовой базы и установка политики информационной безопасности страны в соответствии с международными стандартами;
в) установление спецификаций и стандартов на оборудование и программы для защиты государственных учреждений;
г) разработка политики для решения проблем информационной безопасности в кратчайшие сроки при их возникновении и уменьшении их последствий;
д) распространение информации и культуры информационной безопасности для всех отраслей и пользователей;
е) выполнение тестов проверки качества защиты сетей и систем;
ж) непрерывный поиск новых разработок в области специализации для выдвижения технологий, которые можно приобрести для улучшения условий труда и производства;
з) внедрение систем шифрования, обеспечивающих высокий уровень безопасности информации и данных при сохранении гибкости в их потоке и обращении;
и) предоставление необходимых средств для обеспечения безопасной среды для электронных транзакций между государственными учреждениями, а также между гражданами и различными сторонами;
к) обеспечение выдающегося положения Ливии в области информационной безопасности на региональном, континентальном и международном уровнях;
л) обеспечение безопасности информации и систем для предотвращения несанкционированного доступа.

3.2. Министерство связи и информатики[5]

Министерство занимается вопросами связи и информационных технологий и является высшим органом, ответственным за телекоммуникационный сектор в Ливии. Его штаб-квартира находится в городе Триполи. Оно смогло добиться многих успехов, соединив различные регионы Ливии после того, как инфраструктура связи была нарушена и подвергалась саботажу в месяцы революции. Функции Министерства:

1) подготовка проектов законов и нормативных актов, относящихся к секторам ИКТ и почтовой связи;

5 https://www.cim.gov.ly/

2) контроль исполнения законодательства, касающегося данного сектора;
3) разработка национальных планов и контроль за их выполнением;
4) разработка национального плана использования частотного спектра, управление и распределение использования радиочастот;
5) организация взаимосвязи между сетями связи на основе предоставления услуг;
6) выдача лицензий и установка сборов за все виды лицензий, связанных с деятельностью в сфере ИКТ;
7) предложение правил предоставления лицензий;
8) установление контроля за определением цен и сборов за предоставление услуг;
9) определение минимального качества и уровня предоставления услуг;
10) установка технических и нормативных спецификаций для коммуникационных и информационных систем для всех государственных учреждений;
11) установка стандартов и контроль некоммерческих телекоммуникационных услуг для удаленных районов с определением обязательств операторов и поставщиков услуг;
12) анализ и оценка необходимости изменения уровня организации службы и предложение соответствующих решений;
13) поощрение инвестиций в сектор и создание для них соответствующих условий;
14) мониторинг, надзор и контроль за деятельностью сектора и мониторинг компаний, работающих в секторе;
15) мониторинг спутниковых проектов и внедрение соответствующего законодательства;
16) установка контроля и стандартов, связанных с национальной безопасностью в секторе, в координации с соответствующими органами власти;
17) изучение международных договоров и соглашений, которые относятся к сектору, предложение участия или присоединения к ним и контроль за их выполнением;
18) участие в международных организациях, посещение региональных и международных конференций и семинаров, представление своих решений и рекомендаций на утверждение и контроль за их выполнением;
19) представление государства в международных организациях в области связи и информационных технологий в координации с соответствующими органами власти;
20) содействие конкуренции в сфере предоставления услуг и предотвращение незаконной конкуренции; принятие всех законных мер против нарушений в этой области;

21) сбор информации, которая касается сектора, подготовка и публикация отчетов, необходимых для ориентации получателей услуг, а также внесение вклада в программы СМИ для повышения осведомленности общественности в этой области.

4. Участие в международном сотрудничестве в области формирования системы обеспечения международной информационной безопасности в рамках ООН и позиция при голосовании по наиболее важным резолюциям ГА ООН

Ливия поддержала российский проект резолюции Генеральной Ассамблеи ООН от 5 декабря 2018 г. A/RES/73/27 о переформатировании дискуссии по МИБ в прозрачный, инклюзивный диалог и созыве РГОС.

Резолюция Генеральной Ассамблеи ООН A/RES/73/187 «Противодействие использованию информационно-коммуникационных технологий в преступных целях» от 17 декабря 2018 г. была поддержана.

Ливия одобрила американский проект резолюции Генеральной Ассамблеи ООН «Поощрение ответственного поведения государств в киберпространстве в контексте международной безопасности» (A/RES/73/266 от 22 декабря 2018 г.).

5. Участие в международном сотрудничестве с другими международными организациями в области формирования системы обеспечения информационной безопасности на региональном уровне

5.1. Сотрудничество в сфере реагирования на инциденты

Национальное управление информационной безопасности и охраны (NISSA) поддерживает постоянную связь со своими партнерами как в частном, так и в государственном секторе с целью консолидации всех усилий, направленных на обеспечение безопасности и сохранности информации. Одновременно управление поддерживает связь со многими организациями, связанными с командами реагирования на компьютерные чрезвычайные ситуации. Оно является членом объединения групп реагирования Организации исламского сотрудничества (IOC-CERT), а также одним из основателей регионального AfricaCERT. Также управление работает над тем, чтобы стать эффективным членом глобального форума групп реагирования FIRST.

5.2. Сотрудничество с МСЭ и ARCC

Команда NISSA принимала участие в региональном семинаре по оценке готовности к экстренному информационному реагированию, который состоялся

в столице Катара Дохе в 2017 году. Семинар был спонсирован МСЭ и Арабским региональным центром кибербезопасности (ARCC), а также Министерством связи и коммуникаций Катара. Целью данного семинара было расширение коммуникационных возможностей и повышение потенциала групп реагирования на чрезвычайные ситуации в информационной сфере для обеспечения непрерывных усилий по противодействию киберугрозам в информационной сфере для арабского региона.

6. Содержание и оценка предложений и инициатив в области формирования системы обеспечения международной информационной безопасности

Ливийских предложений и инициатив по указанному направлению деятельности не выявлено.

13. МАВРИТАНИЯ

Официальное название: Исламская Республика Мавритания

Столица: Нуакшот

Официальный язык: арабский

Территория: 1 030 700 км² (28-я в мире). Мавритания граничит с Алжиром, Мали, Западной Сахарой и Сенегалом. С запада омывается Атлантическим океаном (около 700 км береговой полосы). Более 60% территории страны занимают каменистые и песчаные пустыни западной Сахары, территория в основном равнинная — высота до 915 м (гора Кедиет Иджил), хотя встречаются и живописные останцовые скальные массивы. Низшие точки страны — до 5 м ниже уровня моря.

Население: 3 631 775 чел. (по оценкам на 2015 год), что является 131-м показателем в мире.

Государственное устройство: Мавритания является исламской республикой. По конституции, принятой в 1991 году, глава государства — президент, избираемый населением на пятилетний срок.

Парламент — двухпалатный: Сенат (56 мест) избирается на шестилетний срок (треть сенаторов должна обновляться каждые два года), Национальное собрание (95 депутатов) избирается на пятилетний срок.

Экономика: Показатели ВВП (Паритет покупательной способности) за 2018 год:

- Итого: $22,736 млрд (143-й показатель в мире)
- На душу населения: $5727 (130-й показатель в мире)

Показатели ВВП (Номинал) за 2018 год:

- Итого: $7,048 млрд (147-й показатель в мире)
- На душу населения: $1775 (160-й показатель в мире)

Дипломатические отношения с Россией (СССР): установлены 12 июля 1964 г.

1. Уровень развития системы обеспечения информационной безопасности и информационно-коммуникационной инфраструктуры (включая индекс развития ИКТ по оценкам МСЭ и ООН)

По данным МСЭ, с 2002 года позиция Мавритании в глобальном рейтинге оставалась достаточно стабильной. Лучший результат был в 2008 году — 126-я позиция, в 2021 году государство заняло в рейтинге 131-е место, что ниже среднего показателя среди государств-членов ЛАГ.

Страна остается слабоинформатизированной, уровень проникновения Интернета в настоящее время составляет 11,3%. Соответственно, интегральный индекс кибербезопасности Мавритании, рассчитанный МСЭ с учетом развития правовой системы обеспечения информационной безопасности, технических и организационных мер, реализации программ наращивания потенциала и участия в международном сотрудничестве, в 2021 году составил всего 18,94 (из 100). Это существенно ниже общемирового показателя. Уровень развития электронного правительства в стране находится на среднем уровне, тем не менее индекс электронного участия значительно ниже общемирового[1].

2. Нормативно-правовая база в сфере обеспечения информационной безопасности

2.1. Закон о киберпреступности (2016)

Закон о киберпреступности[2] направлен на обеспечение стандартов приемлемого поведения для пользователей информационных и коммуникационных технологий, и это соответствует международным стандартами. Кроме того, Закон о киберпреступности определяет правонарушения и предусматривает наказания за нарушения, что также является важным аспектом международных стандартов по киберпреступности.

Компьютерные преступления криминализированы в главе 2 «Преступления против конфиденциальности, целостности и доступности данных и компьютерных систем». Статьи 4-13 предусматривают наказания за различные нарушения: нарушение конфиденциальности компьютера и/или хранящихся на нем данных, нарушения целостности и доступности компьютера, использование/распространение технологий/устройств, которые могут быть использованы для совершения компьютерных преступлений.

1 https://publicadministration.un.org/egovkb/Portals/egovkb/Documents/un/2020-Survey/2020%20UN%20E-Government%20Survey%20-%20Russian.pdf

2 http://tic.gov.mr/IMG/pdf/loi_2016_-_007_relative_la_cybercriminalite.pdf

2.2. Закон о защите данных (2017)

Закон[3] состоит из 101 статьи. Основополагающие принципы обработки персональных данных включают:

1) сбор, обработка и хранение персональных данных должны быть законными, справедливыми и немошенническими;
2) данные должны собираться только для определенных, конкретных и законных целей. Они не могут впоследствии обрабатываться способом, несовместимым с целями, для которых они были первоначально собраны;
3) данные должны быть приемлемыми и актуальными по отношению к целям, для которых они были собраны и обработаны;
4) данные не могут храниться в течение периода, превышающего время, необходимое для целей, для которых они были собраны или обработаны;
5) персональные данные должны быть точными и обновляться по мере необходимости, ошибочные или неполные данные должны быть удалены или исправлены;
6) обработка данных может осуществляться только в соответствии с принципом прозрачности со стороны контролера;
7) персональные данные должны быть конфиденциальными и защищены в соответствии с Законом, особенно если данные передаются по сети;
8) персональные данные могут обрабатываться только при наличии письменного юридического соглашения между сторонами.

3. Основные документы стратегического планирования в области обеспечения информационной безопасности

3.1 Национальная стратегия кибербезопасности

Цели Стратегии[4] направлены на обеспечение безопасности национальной критической инфраструктуры и особенно разрабатываемых электронных услуг, обеспечение предприятий средствами защиты, содействие кибербезопасности, обновление правовой базы и повышение осведомленности пользователей. В Стратегии также заявляется о развитии сотрудничества между заинтересованными сторонами для обеспечения безопасности информационных систем, о повышении качества телекоммуникационных и ИТ-услуг, о борьбе с киберпреступностью и развитии потенциала страны по реагированию на крупные инциденты.

Для достижения указанных целей Стратегии были определены стратегические направления, проанализированные совместно с различными заинтересованными сторонами:

3 http://tic.gov.mr/IMG/pdf/imp1fr-2.pdf
4 http://www.tic.gov.mr/IMG/pdf/strat-cybersecu-mauritanie300519.pdf

а) защита национальных информационных систем и государственных систем;
б) защита критической инфраструктуры;
в) развитие навыков и осведомленности;
г) разработка нормативно-правовой базы;
д) развитие государственно-частного партнерства и международного сотрудничества.

Стратегия также призывает к созданию модели управления для инициирования многоотраслевой активности и обеспечения надлежащей реализации проектов кибербезопасности. Эта модель должна быть основана на создании управленческого органа высокого уровня, ответственного за утверждение и принятие планов действий, национального агентства по кибербезопасности и группы реагирования на чрезвычайные компьютерные ситуации (CERT), не забывая о других оперативных структурах, которые неявно участвуют во всех национальных усилиях.

4. Основные угрозы информационной безопасности и общие подходы к противодействию этим угрозам, в том числе основные направления обеспечения информационной безопасности, включая используемые ключевые институты и инструменты защиты

В Стратегии кибербезопасности Мавритании для обеспечения различных заинтересованных сторон средствами защиты выделены угрозы, в основном связанные с возможными атаками на КИИ, атаками вредоносных программ, атаками на базы персональных данных граждан и банковским мошенничеством. В документе отдельно выделяется такая угроза, как отсутствие экспертов в области кибербезопасности. Об этой угрозе заявили несколько заинтересованных сторон Мавритании, отмечая отсутствие компаний или экспертов, которые могли бы помочь восполнить недостаток кадров или проконсультировать отдельных специалистов. Столкнувшись с такой проблемой, компании не могут справиться с различными задачами по обеспечению безопасности своих информационных систем. Этот недостаток, как правило, объясняется отсутствием академической подготовки и недостаточностью профессиональной подготовки.

4.1. Главное управление ИКТ (DGTIC)

Главное управление информационных и коммуникационных технологий[5] является центральным управлением Министерства занятости, профессионального обучения и ИКТ, в его обязанности входит:

а) разработка и реализация государственной политики в области информационных и коммуникационных технологий, включая телекоммуникации и почту;

5 https://www.godan.info/organizations/direction-g-n-rale-des-technologies-de-linformation-et-de-la-communication-dgtic

б) обеспечение проектного управления ИТ-проектами, а также делегированное управление проектами отраслевого характера;
в) осуществление и продвижение по согласованию с заинтересованными администрациями действий, позволяющих получить согласованную систему обработки и распространения информации, отвечающую международным стандартам с точки зрения качества, безопасности, производительности и доступности.

4.2. Мавританская обсерватория связи и ИКТ

Цель: информирование о выборе политики и мониторинг реализуемых стратегий. Основными задачами структуры являются[6]:

а) дать возможность соответствующим администрациям и регулятору иметь единую точку доступа к информации, необходимой для выполнения их миссий, на региональном и национальном уровнях;
б) предоставить набор структурированной информации, которая позволяет охарактеризовать место телекоммуникаций и ИКТ в экономике Мавритании;
в) содействовать оценке, совершенствованию и коммуникации инициатив в области телекоммуникаций и ИКТ;
г) способствовать развитию телекоммуникаций и ИКТ как на национальном (частные лица, предприятия, администрации), так и на международном уровне (инвесторы, международные организации и т.д.).

Для реализации последней задачи задачи используются следующее:

а) предоставление операторам, инвесторам и другим заинтересованным организациям набора общей информации о рынках, позволяющей им ориентировать свои действия на лучшее удовлетворение потребностей рынка;
б) путем предоставления международным спонсорам возможности контролировать поддерживаемые проекты и проверять соблюдение установленных этапов;
в) предоставления субрегиональным и международным учреждениям (МСЭ, Всемирный банк, ЭКОВАС, UMA и т.д.) информации и аналитических материалов по сектору ИКТ для их конкретных нужд.

5. Участие в международном сотрудничестве в области формирования системы обеспечения международной информационной безопасности в рамках ООН и позиция при голосовании по наиболее важным резолюциям ГА ООН

Исламская Республика Мавритания поддержала российский проект резолюции Генеральной Ассамблеи ООН от 5 декабря 2018 г. A/RES/73/27 о перефор-

6 http://observatoire.gov.mr/

матировании дискуссии по МИБ в прозрачный, инклюзивный диалог и созыве РГОС).

Резолюция Генеральной Ассамблеи ООН A/RES/73/187 «Противодействие использованию информационно-коммуникационных технологий в преступных целях» от 17 декабря 2018 г. страной была поддержана.

Мавритания одобрила американский проект резолюции Генеральной Ассамблеи ООН «Поощрение ответственного поведения государств в киберпространстве в контексте международной безопасности» (A/RES/73/266 т 22 декабря 2018 г.).

6. Участие в международном сотрудничестве с другими международными организациями в области формирования системы обеспечения информационной безопасности на региональном уровне

6.1. Сотрудничество в рамках G5 Sahel (2018)

В рамках поддержки агентов служб кибербезопасности, киберпреступности и кибертерроризма стран G5 Sahel[7] в 2018 г. проведен Региональный семинар по киберпреступности «Кибертеррористы в странах G5 Sahel». В нем приняли участие 18 агентов служб кибербезопасности, киберпреступности и кибертерроризма Нигера, Мали, Буркина-Фасо, Мавритании и Чада, эксперты платформ киберпреступности Кот-д`Ивуара и Сенегала, а также представители Постоянного секретариата G5 Sahel, УНП ООН, Европола и Франции.

6.2. Сотрудничество с Советом Европы (2018)

Бюро программы по киберпреступности Совета Европы (C-PROC) организовало визит высокого уровня в Мавританию с целью анализа национального законодательства страны по киберпреступности на предмет соответствия международным стандартам, включая права человека и принципы верховенства закона[8].

Второстепенной задачей миссии была оценка потребностей мавританских властей в наращивании потенциала в области киберпреступности. Мавританские коллеги проявили большой интерес к совершенствованию национального законодательства и его применению с учетом возможного будущего присоединения к Будапештской конвенции, по мнению западных стран, наиболее актуальному международному соглашению по киберпреступности и электронным доказательствам.

7 https://nigerinter.com/2018/04/26/des-experts-partagent-leurs-experiences-a-niamey-pour-combattre-la-cybercriminalite-cyberterrorisme-dans-les-pays-du-g5-sahel/

8 https://www.coe.int/en/web/cybercrime/-/cybercrime-octopus-assessing-mauritania-s-cybercrime-legislation-and-capacities

7. Содержание и оценка предложений и инициатив в области формирования системы обеспечения международной информационной безопасности

Несмотря на некоторые проекты внутренней политики по поддержке инноваций и продвижении стартапов в области ИКТ и информационной безопасности, инициатив в области МИБ не выявлено.

Оценивая уровень развития политики Исламской Республики Мавритания в сфере ИКТ и информационной безопасности, можно говорить о практически полном отсутствии механизма обеспечения информационной безопасности. Принятие и обнародование законов по этому вопросу не принесли большой пользы, и они не исполняются должным образом. Декларируемые в Стратегии задачи и приоритеты хотя и являются важными и в некоторой степени рабочими, но за три года существования документа так и не были выполнены. В Стратегии предлагается формирование Национального агентства кибербезопасности, но оно откладывается. Функции нового управленческого органа выполняет Главное управление ИКТ (DGTIC).

14. МАРОККО

Официальное название: Королевство Марокко

Столица: Рабат

Официальные языки: арабский и берберский

Территория: 446 550 км² (57-я в мире). Омывается на севере водами Средиземного моря и на западе — Атлантического океана. Гибралтарский пролив отделяет Марокко от либо от материка Евразия. На востоке и юго-востоке граничит с Алжиром, на юге — с Западной Сахарой. Юго-восточная граница в пустыне Сахара точно не определена. Общая протяженность сухопутной границы — 2 018 км, в том числе с такими странами как Алжир — 1 559 км, Западная Сахара (оккупирована Марокко) — 443 км, Испания (Сеута) — 6,3 км, Испания (Мелилья) — 9,6 км. Береговая линия страны: 1 835 км.

Население: 37 232 190 чел. (по оценкам на 2023 год), что является 41-м показателем в мире.

Государственное устройство: Марокко — дуалистическая монархия, что закреплено в конституции. Исключительная власть сосредоточена в руках короля и его Совета министров. Король подписывает все законы, его право вето может быть преодолено двумя третями голосов обеих палат Национальной Ассамблеи. Он является духовным главой, символом единства нации, назначает всех судей своими указами, утверждает изменения в конституцию, объявляет войну и командует вооруженными силами. Правительство, возглавляемое премьер-министром, назначается королем, который может освободить от занимаемой должности отдельных министров по запросу премьер-министра.

Конституция предусматривает три вида судов: гражданские, религиозные и специальные. Королевские вооруженные силы также находятся под контролем короля.

Высший орган законодательной власти — двухпалатный парламент. Нижняя палата — Палата представителей (325 депутатов) избирается прямым голосованием на пять лет, верхняя палата — Палата советников (270 депутатов) избирается на девять лет непрямым голосованием. Каждые три года ее состав обновляется на треть.

Экономика: Показатели ВВП (Паритет покупательной способности) за 2019 год:

- Итого: $289,954 млрд (57-й показатель в мире)
- На душу населения: $8148 (121-й показатель в мире)

Показатели ВВП (Номинал) за 2019 год:

- Итого: $118,567 млрд (58-й показатель в мире)
- На душу населения: $3332 (126-й показатель в мире)

Дипломатические отношения с Россией (СССР): установлены 1 сентября 1958 г.

1. Уровень развития системы обеспечения информационной безопасности и информационно-коммуникационной инфраструктуры (включая индекс развития ИКТ по оценкам МСЭ и ООН)

Исходя из перечисленных ниже статистических данных, уровень развития системы информационной безопасности Марокко может быть оценен как средний:

МСЭ 2021, индекс кибербезопасности: 82,41 (из 100)
МСЭ 2021, позиция в рейтинге среди государств-членов ЛАГ: 7
МСЭ 2021, позиция в глобальном рейтинге: 50
МСЭ, уровень проникновения Интернет: 68,5%
NCSI, уровень цифрового развития: 46,88
NCSI, индекс готовности к киберугрозам и реагированию на них: 23,38

2. Основные документы стратегического планирования в области обеспечения информационной безопасности

Закон № 03.07 о контроле автоматизированных систем обработки данных принят в 2003 году в рамках Уголовного кодекса (разделы 3/607–11/607), регулирует противодействие использованию ИКТ в преступных целях. Основные положения разработаны на основе международных конвенций, в первую очередь Конвенции Совета Европы о киберпреступности 2001 года (Будапештская конвенция) и Дополнительного протокола к ней.

Закон № 136.12 об одобрении Конвенции о киберпреступности введен в действие Королевским указом № 1.14.85 от 12 мая 2014 г.

Закон № 12.17 об одобрении Арабской конвенции о борьбе с преступлениями в области информационных технологий введен в действие Королевским указом № 46.13.1 от 13 марта 2013 г.

Закон № 108.13 о военной юстиции (статья 3) предусматривает определенные требования, касающиеся преступлений, которые подпадают под юрисдикцию военного суда, что позволяет этому суду также выносить приговоры по делам о киберпреступлениях.

Закон № 53.05 об электронном обмене правовыми данными (направлен на защиту персональных данных или электронного обмена данными) введен в действие Королевским указом № 1.07.129 от 30 ноября 2007 г.

Закон № 09.08 о защите персональных данных (направлен на создание благоприятных условий для инвестиций в сферу информационных технологий и цифровой экономики) введен в действие Королевским указом № 1.09.15 от 18 февраля 2009 г.

Законопроект о борьбе с организованной информационной преступностью — предусматривает инструменты для реагирования на этот вид преступности.

Законопроект о руководящих указаниях по борьбе с преступлениями в области информационных технологий.

Национальная стратегия в области кибербезопасности (разработана в 2012 году в соответствии с Королевским указом № 2-11-508 от 21 сентября 2011 г. «О создании Стратегического комитета по безопасности информационных систем CSSSI») направлена на обеспечение защиты критически важных информационных систем органов власти, государственных учреждений и инфраструктуры.

Стратегические направления Стратегии:

- ✓ оценка рисков для критически важных информационных систем государственных органов, государственных учреждений и инфраструктуры посредством реализации двух программ:
  1) разработка планов оценки рисков и угроз;
  2) внедрение инструментов поддержки принятия решений;
- ✓ защита критически важных информационных систем государственных органов, государственных учреждений и инфраструктуры посредством реализации трех программ:
  1) разработка национальных репозиториев и стандартов;
  2) повышение безопасности критически важных информационных систем государственных органов, государственных учреждений и инфраструктуры;
  3) укрепление структур мониторинга, обнаружения и реагирования на IT-инциденты;
- ✓ укрепление основ безопасности: правовая база, информационно-пропагандистская деятельность, обучение, исследования и разработки посредством реализации четырех программ:
  1) укрепление правовой базы для укрепления цифрового доверия;
  2) определение и организация учебных программ по техническим и правовым вопросам, связанным с кибербезопасностью;
  3) повышение осведомленности о кибер-этике, а также угрозах и рисках, связанных с безопасностью информационных систем;
  4) поддержка исследований и разработок национальных продуктов безопасности информационных систем для обеспечения научно-технической автономии;
- ✓ содействие и развитие сотрудничеству на национальном и международном уровнях посредством реализации двух программ:
  1) определение тем и механизмов сотрудничества;

2) налаживание партнерских отношений и их реализация.

Стратегия «Цифровое Марокко 2013»:

- ✓ цель — поддержание цифрового доверия в целях реализации государственных подходов, согласно которым кибербезопасность рассматривается в качестве необходимой вспомогательной меры для развития в Марокко цифровой экономики;
- ✓ приоритетная задача — адекватное реагирование на человеческий, правовой, экономический и технологический аспекты потребностей цифровой инфраструктуры и пользователей в области информационной безопасности.

Основные направления Стратегии:

- ✓ учет анализа рисков, связанных с киберпространством;
- ✓ определение политической безопасности информационных систем (PSSI) для преобразования понимания возникающих рисков и их последствий в меры безопасности, которые необходимо реализовать;
- ✓ развертывание решений, способных защитить компьютерные системы и телекоммуникационную инфраструктуру;
- ✓ внедрение подходов к обнаружению угроз и реагированию на них;
- ✓ создание надлежащих правовых рамок;
- ✓ поощрение исследований и разработок в области безопасности информационных систем, а также обязательство соблюдать минимальные стандарты;
- ✓ повышение осведомленности всех участников в целях поощрения культуры кибербезопасности.

В процессе совершенствования нормативно-правовой базы в области кибербезопасности приняты Национальная директива по обеспечению безопасности информационных систем и директива «О правилах безопасности и порядке использования информационных систем в ключевых областях» (2017 год).

3. Основные угрозы информационной безопасности и общие подходы к противодействию этим угрозам, в том числе основные направления обеспечения информационной безопасности, включая используемые ключевые институты и инструменты защиты

Проблемы в противодействии киберпреступности в Марокко обусловлены:

- ✓ анонимностью: использование посредников и даркнета;
- ✓ транснациональным характером: хранение доказательств на серверах, расположенных за пределами национальной территории;
- ✓ частым использованием шифрования данных;
- ✓ использованием криптовалюты в преступных целях;

- ✓ постоянным изменением используемых способов деятельности;
- ✓ трудностями в доступе к данным о передвижении пользователей определенных приложений или сайтов, находящихся за границей;
- ✓ планированием постоянной подготовки в области борьбы с киберпреступностью для персонала, участвующего в расследовании киберпреступлений и сборе цифровых доказательств, чтобы не отставать от стремительного развития технологий;
- ✓ приобретением соответствующих и эффективных специальных аппаратных средств и программного обеспечения для расследования киберпреступлений;
- ✓ необходимостью охвата пользователей ИКТ программой повышения осведомленности о рисках несоблюдения мер защиты;
- ✓ введением в действие механизмов защиты от киберугроз и реагирования на них на региональном уровне;
- ✓ межгосударственным сотрудничеством и координацией при уточнении правовых вопросов и осуществлении соответствующего законодательства, а также в процессе деятельности следственных органов и эффективного проведения расследования с использованием цифровых доказательств.

Другие проблемы в борьбе с использованием ИКТ в преступных целях:

- ✓ запоздалое реагирование законодательства на быстрое развитие киберпреступности;
- ✓ отсутствие правовой базы для борьбы с преступлениями, совершаемыми с использованием социальных сетей;
- ✓ отсутствие в большинстве действующих правовых норм требований, устанавливающих ответственность поставщиков сетевых услуг и обязывающих их удалять, блокировать, приостанавливать или закрывать доступ к незаконному электронному контенту;
- ✓ отсутствие международного документа, допускающего прямое сотрудничество с поставщиками услуг в других юрисдикциях в целях обеспечения трансграничного взаимодействия для передачи данных.

Государственные органы в области кибербезопасности:

В рамках Национального аппарата безопасности создана целевая группа судебной полиции для борьбы с киберпреступностью (два антитеррористических подразделения для борьбы с преступлениями, связанными с информационными системами, на уровне как расследования, так и розыска преступников через Интернет).

В Министерстве национальной обороны действует Управление по вопросам киберпреступности для расследования киберпреступлений, отслеживания их по-

следствий и борьбы с ними во взаимодействии с различными департаментами национальной и международной безопасности.

Стратегический комитет по безопасности информационных систем (CSSSI)

Главное управление по безопасности информационных систем Министерства национальной обороны (DGSSI).

Национальный совет по медийным технологиям и цифровой экономике общениях, введенному в действие Королевским указом № 1.97.162 от 1 августа 1997 г.) для координации национальной политики и оценки ее реализации.

4. Участие в международном сотрудничестве в области формирования системы обеспечения международной информационной безопасности в рамках ООН и позиция при голосовании по наиболее важным резолюциям ГА ООН

Следует отметить, что Марокко было членом ГПЭ шестого созыва (2019–2021), как правило, поддерживает российские инициативы в области международной информационной безопасности, голосуя за их принятие.

В 2018–2020 годах проголосовал в поддержку российских проектов резолюций Генеральной Ассамблеи ООН:

A/RES/73/27 от 5 декабря 2018 г. (принятие правил, норм и принципов ответственного поведения, а также создание Рабочей группы ООН открытого состава);

A/RES/73/187 от 17 декабря 2018 г. (включение в повестку дня ООН обсуждения вопроса о противодействии использованию ИКТ в преступных целях);

A/RES/75/240 от 31 декабря 2020 г. (создание новой Рабочей группы ООН открытого состава по вопросам безопасности в сфере использования ИКТ и самих ИКТ 2021–2025).

Вместе с тем Марокко воздержалось при голосовании по российскому проекту резолюции Генеральной Ассамблеи ООН:

A/RES/74/247 от 27 декабря 2019 г. (создание специального межправительственного комитета экспертов открытого состава для разработки всеобъемлющей международной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях).

Проголосовало за принятие американского проекта резолюции Генеральной Ассамблеи ООН A/RES/73/266 от 22 декабря 2018 г. (о создании Группы правительственных экспертов ООН на 2019–2021 годы).

5. Участие в международном сотрудничестве с другими международными организациями в области формирования системы обеспечения информационной безопасности на региональном уровне

Марокко взаимодействует на глобальном и региональном уровнях по вопросам обеспечения кибербезопасности в рамках следующих международных организаций, членом которых оно является:

ООН;

ITU (МСЭ);

Движение неприсоединения;

Африканский союз;

ЛАГ;

Интерпол;

ISO (Международная организация по стандартизации).

В 2014 году Марокко стало участником Европейской конвенции по киберпреступлениям.

6. Содержание и оценка предложений и инициатив в области формирования системы обеспечения международной информационной безопасности

Марокко:

присоединилось к инициативе Франции — Парижский призыв к доверию и безопасности в киберпространстве (2018 год);

стало соавтором инициативы Франции и Египта — Программа действий ООН по продвижению ответственного поведения государств в киберпространстве (2020 год).

15. ОАЭ

Официальное название: Объединенные Арабские Эмираты

Столица: Абу-Даби

Официальный язык: арабский

Территория: 82 880 км² (114-я в мире). Объединенные Арабские Эмираты занимают территорию на северо-восточном окончании Аравийского полуострова. ОАЭ граничат с Саудовской Аравией на юге и западе и с Оманом на востоке. Северное побережье находится напротив Ирана через Персидский залив, в то время как Катар — всего в 50 км к северо-западу. ОАЭ состоят из семи эмиратов — Абу-Даби, Аджман, Дубай, Фуджейра, Рас-эль-Хайма, Шарджа и Умм-эль-Кайвайн. Вместе эти эмираты занимают территорию примерно таких же размеров, как Португалия.

Население: 9 771 000 чел. (по оценкам на 2019 год), что является 92-м показателем в мире.

Государственное устройство: Государственное устройство Объединенных Арабских Эмиратов представляет собой уникальное сочетание республиканского и монархического строя. ОАЭ являются федеративным монархическим государством, состоящим из семи эмиратов — абсолютных монархий. Государство возглавляется эмиром Абу-Даби, правительство — эмиром Дубая.

Высший совет союза занимает первенствующее место в иерархии государственного устройства ОАЭ. Совет состоит из глав всех семи эмиратов. Совет определяет общую политику государства, а Совет министров отвечает перед Высшим советом за проведение этой политики. Помимо определения внешней и внутренней политики Высший совет вправе пересматривать принцип государственного устройства страны. Совет также утверждает кандидатуру на пост председателя Совета министров.

Пост президента Объединенных Арабских Эмиратов совмещен с постом эмира столичного эмирата Абу-Даби. Так как сам эмират является абсолютной монархией, то власть в нем, а, следовательно, и во всем государстве, передается по наследству. До 1966 года в Абу-Даби, как и в соседней Саудовской Аравии, было принято передавать власть от брата к брату. Президент ОАЭ является верховным главнокомандующим вооруженными силами, председателем Высшего совета обороны. Глава государства подписывает указы и постановления, подтвержден-

ные Высшим советом, нормативные акты, принятые Советом министров. Кроме того, президент назначает членов дипломатического корпуса, высших гражданских и военных чиновников, объявляет амнистию либо подтверждает смертные приговоры.

Исполнительная власть представлена Советом министров во главе с председателем, назначаемым на пост президентом и утверждаемым Высшим советом. К полномочиям правительства относятся разработка законопроектов и федерального бюджета, принятие постановлений и инструкций для исполнения законов и других нормативных актов, наблюдение за исполнением судебных решений, ратификация международных договоров и соглашений, назначение и увольнение федеральных чиновников, которые не требуют особого распоряжения других высших органов государства.

Экономика: Показатели ВВП (Паритет покупательной способности) за 2019 год:

- Итого: $683,523 млрд (34-й показатель в мире)
- На душу населения: $63 590 (8-й показатель в мире)

Показатели ВВП (Номинал) за 2019 год:

- Итого: $421,142 млрд (29-й показатель в мире)
- На душу населения: $39 180 (25-й показатель в мире)

Дипломатические отношения с Россией (СССР): установлены 8 декабря 1971 г.

1. Уровень развития системы обеспечения информационной безопасности и информационно-коммуникационной инфраструктуры (включая индекс развития ИКТ по оценкам МСЭ и ООН)

Исходя из перечисленных ниже статистических данных, уровень развития системы информационной безопасности ОАЭ может быть оценен как высокий:

МСЭ 2021, индекс кибербезопасности: 98,06 (из 100)

МСЭ 2021, позиция в рейтинге среди государств-членов ЛАГ: 2

МСЭ 2021, позиция в глобальном рейтинге: 5

МСЭ, уровень проникновения Интернет: 103,3%

NCSI, уровень цифрового развития: 68,01

NCSI, индекс готовности к киберугрозам и реагированию на них: 40,26

2. Основные документы стратегического планирования в области обеспечения информационной безопасности

Национальная стратегия кибербезопасности утверждена в 2019 году Регуляторным органом телекоммуникаций (TRA) и содержит:

- принципы обеспечения кибербезопасности;
- инициативы, направленные на мобилизацию всей системы кибербезопасности в стране.

Принципы обеспечения кибербезопасности определенно:

- ✓ внедрение комплексной нормативно-правовой базы, которая будет охватывать все виды киберпреступлений, защищать существующие и новые технологии от кибератак, а также помогать малому и среднему бизнесу в обеспечении информационной безопасности;
- ✓ мобилизация экосистемы кибербезопасности страны путем развития рынка кибербезопасности (который, согласно оценкам, данным в Стратегии, составляет около 500 млн США), расширения возможностей более 40 тыс. экспертов в области кибербезопасности, поощрения образовательных мероприятий и продвижения карьеры в данной сфере, повышения осведомленности граждан о кибербезопасности, а также поощрения достижений в области информационной безопасности с помощью национальных программ;
- ✓ создание национального плана реагирования на компьютерные инциденты;
- ✓ защита важнейших активов ОАЭ в таких секторах, как энергетика, ИКТ, правительство, электричество и водообеспечение, финансы и страхование, экстренные службы, медицина, транспорт, продовольствие и сельское хозяйство;

- ✓ развитие местных и глобальных партнерств для совместного достижения целей кибербезопасности, потенциала государственно-частного партнерства.

Инициативы по обеспечению кибербезопасности:

- ✓ развитие малого и среднего бизнеса в указанной сфере;
- ✓ поддержка инновационных проектов и НИОКР;
- ✓ стандартизация методик и планов по обеспечению кибербезопасности;
- ✓ развитие систем активного мониторинга кибербезопасности и др.

Закон управления медицинской информацией принят в 2019 году Президентом ОАЭ. Основное предназначение:

- ✓ регулирует сбор, обработку и передачу электронных данных о состоянии здоровья пациентов в целях максимальной защиты персональных медицинских данных и обеспечения эффективной системы сбора и анализа медицинской информации;
- ✓ распространяется на все организации, работающие на территории страны, которые предоставляют медицинское оборудование, услуги медицинского страхования и любые другие услуги, прямо или косвенно связанные с данным сектором;
- ✓ регулирует обработку всех электронных медицинских данных независимо от их формы, включая имена пациентов, информацию о консультациях, диагностиках и расписаниях лечения и т.д.;
- ✓ предусматривает, что медицинские данные не могут передаваться за пределы страны, что приводит ограничения на использование международных облачных сервисов;
- ✓ планирует создание централизованной системы управления медицинскими данными для облегчения доступа к ним и обмена информацией, а также внедрение специальных алгоритмов идентификации медицинского персонала для обеспечения защиты данной платформы;
- ✓ предусматривает возможность анонимизации медицинской информации.

Стратегия кибербезопасности Дубая принята в 2017 году Правительством Дубая и Центром электронной безопасности Дубая, нацелена на снижение вероятности проявления таких киберугроз, как мошенничество в сети, кибершпионаж, нарушение приватности информации, кибертерроризм и дезинформация.

<u>Ключевые принципы данной Стратегии</u>:

- ✓ обеспечение открытости информации;
- ✓ управление рисками в области кибербезопасности;
- ✓ обеспечение взаимодействия государственного и частного секторов в целях защиты критической инфраструктуры;

- ✓ обеспечение соответствия законодательству в области информационной безопасности.

Ключевые цели Стратегии:

- ✓ повышение осведомленности в области кибербезопасности населения путем разработки образовательных мероприятий, распространения практик по кибербезопасности, повышения квалификации специалистов данной области и др.;
- ✓ инновационное развитие в сфере информационной безопасности, применение технологий искусственного интеллекта, обеспечение взаимодействия для проведения исследований и разработок;
- ✓ распределение ответственности за обеспечение кибербезопасности;
- ✓ обеспечение киберустойчивости информационной инфраструктуры страны;
- ✓ международное взаимодействие в сфере кибербезопасности.

Политика управления данными Дубая обновлена в 2017 году Офисом «умного» города Дубай: введены основные термины и определения в области информационной безопасности, а также распределена ответственность по управлению данными.

Ключевой элемент политики Дубая в области информационной безопасности — политика открытых данных.

В данном документе выделяются следующие технологии и методы в области обеспечения защиты данных:

- ✓ использование облачных платформ для взаимообмена данными в государственных системах между правительственными органами;
- ✓ внедрение элементов авторизации для обеспечения конфиденциальности информации;
- ✓ ограничение доступа к данным в государственных информационных системах;
- ✓ использование алгоритмов классификации и систематизации информации;
- ✓ оценка рисков утечки персональных данных;
- ✓ установление ключевых показателей эффективности в области кибербезопасности и др.

Федеральный закон о борьбе с киберпреступностью принят в 2012 году взамен Федерального закона о борьбе с преступлениями в сфере информационных технологий 2006 года, регулирует злоупотребление и неправомерное использование электронной информации посредством таких действий, как взлом, кража личных данных и мошенничество.

3. Основные угрозы информационной безопасности и общие подходы к противодействию этим угрозам, в том числе основные направления обеспечения информационной безопасности, включая используемые ключевые институты и инструменты защиты

Основные направления обеспечения кибербезопасности:

- ✓ обеспечение безопасности информационной инфраструктуры и сети Интернет;
- ✓ объединение усилий между государством, научной сферой и бизнесом для обеспечения кибербезопасности;
- ✓ разработка инновационных решений в области кибербезопасности.

Правила для владельцев веб-сайтов и услуг в сети (в 2019 году были обновлены), которые обязывают администраторов веб-сайтов обеспечить их соответствие следующим положениям:

- ✓ содержание сайта не должно включать в себя ни одну из категорий запрещенного контента (порнография, дезинформация, фишинговые ссылки и др.), а также должно соответствовать законодательным нормам;
- ✓ сайт должен иметь эффективный механизм доступа пользователей к информации о владельцах сервиса;
- ✓ должны быть сформированы положения конфиденциальности с указанием того, какая персональная информация пользователей будет собрана и в каких целях;
- ✓ необходимо обеспечить сбор информации безопасным способом (например, с использованием технологий SSL-шифрования);
- ✓ необходимо оборудовать серверы веб-сайтов инструментами защиты (установка антивирусного программного обеспечения, проведение аудита безопасности и др.);
- ✓ необходимо блокировать доступ к материалам, нарушающим авторские права, обеспечивать безопасный поиск информации с инструментами ее фильтрации и др.

Проекты по цифровизации, реализуемые в ОАЭ государственными и коммерческими организациями, а также объединениями организаций

Цифровая безопасность детей — реализуемая с конца 2018 года инициатива, регламентирующая образовательные мероприятия по повышению осведомленности детей об угрозах в сети Интернет, а также по ознакомлению родителей и преподавателей с решениями, которые можно использовать для защиты детей

в Интернете (обеспечивается за счет разработки учебных материалов по цифровой безопасности в соответствии с лучшими мировыми практиками, а также консультирования родителей и учителей в области безопасности детей в сети как дома, так и в учебной среде).

Меры по реализации данной инициативы:

- ✓ создание интерактивной площадки для детей от 5 до 18 лет, где они могут научиться безопасно пользоваться Интернетом и социальными сетями;
- ✓ внедрение специализированного портала, который описывает инструменты для использования родителями в целях обеспечения защиты персональной информации детей;
- ✓ учебные семинары, на которых происходит обучение родителей и учителей по решению проблем и устранению угроз, связанных с цифровой безопасностью;
- ✓ создание платформы поддержки для реагирования на инциденты кибербезопасности детей и консультаций по вопросам цифровой безопасности.

Органы, ответственные за обеспечение кибербезопасности в ОАЭ:

Головным органом является — Дубайский Центр электронной безопасности — основан в 2014 году с целью разработки и внедрения методов информационной безопасности в ОАЭ;

Национальное управление электронной безопасности (NESA) создано в 2012 году для обеспечения соблюдения Закона о киберпреступности, регулирования защиты сетей связи и информационных систем в ОАЭ, а также для разработки стандартов в сфере сетевой и информационной безопасности, способов и механизмов защиты;

Регулирующий орган электросвязи (TRA) создан в 2003 году для регулирования сектора информационных коммуникаций и телекоммуникаций в ОАЭ, а также для обеспечения устойчивости и конкурентоспособности среди поставщиков услуг, клиентов и инвесторов;

Национальная группа реагирования на компьютерные инциденты (uaeCERT) создана под руководством TRA для обеспечения безопасной киберсреды для всех жителей ОАЭ.

4. Участие в международном сотрудничестве в области формирования системы обеспечения международной информационной безопасности в рамках ООН и позиция при голосовании по наиболее важным резолюциям ГА ООН

ОАЭ поддерживают российские инициативы в области международной информационной безопасности.

В 2018–2020 годах ОАЭ голосовали в поддержку российских проектов резолюций Генеральной Ассамблеи ООН:

A/RES/73/27 от 5 декабря 2018 г. (принятие правил, норм и принципов ответственного поведения, а также создание Рабочей группы ООН открытого состава);

A/RES/73/187 от 17 декабря 2018 г. (включение в повестку дня ООН обсуждения вопроса о противодействии использованию ИКТ в преступных целях);

A/RES/74/247 от 27 декабря 2019 г. (создание специального межправительственного комитета экспертов открытого состава для разработки всеобъемлющей международной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях);

A/RES/75/240 от 31 декабря 2020 г. (создание новой Рабочей группы ООН открытого состава по вопросам безопасности в сфере использования ИКТ и самих ИКТ 2021–2025).

При голосовании за принятие американского проекта резолюции Генеральной Ассамблеи ООН A/RES/73/266 от 22 декабря 2018 г. (о создании Группы правительственных экспертов ООН на 2019–2021 годы) ОАЭ поддержали данный проект.

5. Участие в международном сотрудничестве с другими международными организациями в области формирования системы обеспечения информационной безопасности на региональном уровне

ОАЭ взаимодействуют на глобальном и региональном уровнях по вопросам обеспечения кибербезопасности в рамках следующих международных организаций, членом которых они являются:

ООН;

ITU (МСЭ);

Движение неприсоединения;

ЛАГ;

Интерпол;

ISO (Международная организация по стандартизации).

6. Содержание и оценка предложений и инициатив в области формирования системы обеспечения международной информационной безопасности

ОАЭ присоединились к инициативе Франции — Парижскому призыву к доверию и безопасности в киберпространстве (2018 год), но не выступили соавторами инициативы Франции и Египта — Программы действий ООН по продвижению ответственного поведения государств в киберпространстве (2020 год).

7. Искусственный интеллект, блокчейн-технологии, сети 5G

Искусственный интеллект

Национальная стратегия развития искусственного интеллекта (ИИ) до 2031 года призвана повысить эффективность обслуживания клиентов, автоматизировать работу государственных органов, а также внедрить современные технологии искусственного интеллекта в сектор транспорта, туризма, здравоохранения и образования.

Правительство ОАЭ ставит перед собой глобальную задачу — сделать страну лидером в области технологий искусственного интеллекта к 2031 году, а также разработать и внедрить интегрированную систему на базе технологий искусственного интеллекта в жизненно важных областях экономики ОАЭ.

Новая национальная стратегия включает в себя восемь глобальных целей, а также ряд инициатив, направленных на использование ИИ в таких областях, как образование, транспорт, государственные службы и сфера услуг.

Ключевые задачи, поставленные Правительством:

- укрепить позиции ОАЭ как мирового лидера в области технологий искусственного интеллекта;
- повысить конкурентоспособность сектора ИИ в ОАЭ;
- организовать инновационный инкубатор для внедрения новых технологий искусственного интеллекта;
- внедрить ИИ-технологии в сфере обслуживания клиентов;
- подготовить перспективных специалистов для работы в этом направлении;
- привлечь зарубежные исследовательские группы для разработки и внедрения инноваций в области ИИ;
- организовать возможность проведения масштабных практических экспериментов с использованием искусственного интеллекта и их скорейшего внедрения в реальный сектор экономики;
- оптимизировать управление проектами и регулирование с использованием технологий ИИ.

Согласно новой стратегии на первом этапе реализации усилия будут сосредоточены в следующих областях: энергетика и горнодобывающая промышленность, транспорт и логистика, туризм, здравоохранение и безопасность.

Ожидается, что новые технологии с использованием ИИ значительно увеличат национальный ВВП в ближайшие годы, что создаст новые экономические возможности и позволит экономике ОАЭ продолжить свою диверсификацию.

Блокчейн-технологии

Правительство Объединенных Арабских Эмиратов сотрудничает с Bitcoin Association и представителями экосистемы BSV, чтобы лучше понять значение технологии блокчейн и потенциал ее применения для преобразования системы государственного управления страны.

Переговоры с представителями Bitcoin Association и информационно-аналитическое партнерство — это элементы более обширной амбициозной стратегии правительства ОАЭ по цифровизации.

В рамках стратегии интеграции блокчейна, основанной на четких указаниях правительства, ОАЭ сотрудничает с Центром BSV на Ближнем Востоке и в Южной Азии (регион MESA) для запуска разнообразных образовательных проектов в сфере блокчейна с целью стимулирования инноваций в ОАЭ. Главой находящегося в Дубае Центра BSV в регионе MESA является Мухаммад Салман Анджум, один из лидеров сферы корпоративного блокчейна в регионе и главный исполнительный директор InvoiceMate — платформы следующего поколения для бухгалтерского учета и выставления счетов, которая интегрирована с блокчейном BSV.

Деятельность Центра BSV на Ближнем Востоке и в Южной Азии включает в себя развертывание образовательной программы в ОАЭ, цель которой — познакомить местных разработчиков и предпринимателей с возможностями блокчейна BSV. Эта инициатива уже вызвала большой интерес в стране.

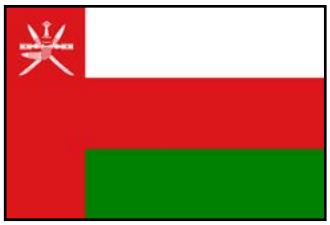
5G в ОАЭ

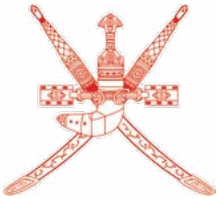
В ОАЭ к концу 2025 года все города и поселения планируют полностью покрыть сетью пятого поколения мобильной связи 5G при помощи выделения вспомогательных частот спектра 24,25–27,5 ГГц. По официальной информации Управления телекоммуникаций ОАЭ, этот шаг будет способствовать укреплению позиций телекоммуникационного сектора Эмиратов и обеспечит нужные ресурсы для международных мобильных коммуникационных приложений.

Полное покрытие ОАЭ мобильной сетью 5G с использованием специальных частот позволит операторам и производителям мобильных устройств создавать совершенно новые сервисы и типы взаимодействия между устройствами. Отмечается, что ОАЭ первыми в регионе MESA открыли доступ к указанным частотам.

Распространение сети пятого поколения значительно повлияет на внедрение новых технологий во многих отраслях экономики и сферах общественной жизни, включая здравоохранение, средства массовой печати, общественный автотранспорт, коммунальные услуги, игровую индустрию, издательское дело и др. Предполагается, что 5G произведет революционные преобразования в способах взаимодействия компании с их клиентами.

16. ОМАН





Официальное название: Султанат Оман

Столица: Маскат

Официальный язык: арабский

Территория: 309 500 км² (70-я в мире). Севернее основной части имеется небольшой полуэксклав Мусандам и его полный эксклав Мадха (один из вилайетов Мусандама), отделенные от основной территории Омана территорией Объединенных Арабских Эмиратов.

На северо-востоке страны вдоль побережья Оманского залива узкой полосой тянется приморская равнина Эль-Батина, наиболее освоенная и плотно заселенная часть страны. Обширное пространство западнее этой равнины занимают горы Хаджар. Отдельные вершины достигают 3000 м (высшая точка — 3020 м). В средней части страны расположено невысокое плато, в значительной степени покрытое песками. Его средние высоты 500 м. В южной части страны, Дофаре, возвышаются горы, наиболее высокие у южного побережья — до 1678 м. Самая восточная точка Омана — Эль-Хадд.

Население: 4 088 690 чел. (по оценкам на 2014 год), что является 127-м показателем в мире.

Государственное устройство: Султанат Оман — абсолютная монархия. Султан Омана является не только главой государства, но и главой правительства, верховным главнокомандующим, министром обороны, иностранных дел и финансов. Султан также назначает кабинет министров. Пост главы государства передается по наследству.

Судебная система Омана регулируется Королевским указом 90/99. В Омане существует три судебных уровня: первичный суд, апелляционный суд, а также Верховный суд в качестве высшей судебной инстанции. Есть административный суд, который рассматривает иски, выдвинутые против правительства.

В ноябре 1991 г. султан Кабус сформировал Консультативную Ассамблею (Меджлис аш-Шура) взамен Государственного совещательного совета, созданного в 1981 году. Меджлис аш-Шура был создан, чтобы расширить и систематизировать участие общественности в управлении государством. Меджлис аш-Шура состоит из 84 членов, осуществляющих некоторые законодательные полномочия. Меджлис аш-Шура служит для связи населения с министерствами и уполномо-

чен рассматривать проекты экономического и социального законодательства, подготовленные службами министерства, и давать рекомендации.

Экономика: Показатели ВВП (Паритет покупательной способности) за 2019 год:

- Итого: $141,558 млрд (78-й показатель в мире)
- На душу населения: $33 748 (43-й показатель в мире)

Показатели ВВП (Номинал) за 2019 год:

- Итого: $76,332 млрд (67-й показатель в мире)
- На душу населения: $18 198 (45-й показатель в мире)

Дипломатические отношения с Россией (СССР): установлены 26 сентября 1985 г.

1. Уровень развития системы обеспечения информационной безопасности и информационно-коммуникационной инфраструктуры

Исходя из статистических данных, уровень развития системы информационной безопасности Султаната Оман один из самых высоких в мире:

МСЭ 2021, индекс кибербезопасности: 96,04 (из 100)

МСЭ 2021, позиция в рейтинге ЛАГ: 3

МСЭ 2021, позиция в глобальном рейтинге: 21

МСЭ, уровень проникновения Интернет: 76,8%

2. Основные документы стратегического планирования в области обеспечения информационной безопасности

2.1. Национальная стратегия «Цифровой Оман и электронное правительство» (e.Oman)

Стратегия e.Oman[1] разрабатывалась под эгидой Министерства транспорта, связи и информационных технологий Султаната Оман. Она направлена на создание в период до 2030 года прочной основы для получения выгод от цифровизации и технологических изменений, обусловленных четвертой промышленной революцией. Стратегические направления e.Oman включают шесть блоков[2].

1. Развитие цифрового общества

- Разработка и внедрение национальной системы обучения и повышения осведомленности в области ИТ.
- Обучение граждан и государственных служащих основам компьютерной грамотности.
- Предоставление школьникам базовых знаний в области ИТ.
- Предложение переподготовки и развитие навыков ИТ для профессионалов.
- Предложение специализированного обучения ИТ и сертификацию ИТ-специалистов.
- Предложение компьютеров и доступ в Интернет населению по сниженным ценам.

2. «Умное» правительство и услуги

- Реинжиниринг идентифицированных процессов.
- Развертывание в государственных организациях, помимо лицензионных пакетов ПО, бесплатных пакетов и с открытым исходным кодом.
- Приобретение и развертывание государственной инфраструктуры, необходимой для предоставления услуг в Интернете.

1 https://www.ita.gov.om/ITAPortal/eOman/eoman.aspx
2 https://www.ita.gov.om/ITAPortal/eOman/Strategic_Pillars.aspx

- Усовершенствование правительственных приложений для предоставления онлайн-услуг.
- Разработка процессов обеспечения непрерывности ИТ-бизнеса для достижения целей восстановления.
- Защита информационных активов правительства.

3. Динамичная экосистема цифровой и ИКТ-индустрии

- Создание большего количества филиалов многонациональных компаний для работы из Омана.
- Управление центрами передового опыта, чтобы способствовать развитию ИТ-индустрии.
- Развитие местной ИТ-индустрии.
- Разработка и продвижение контента и приложений на оманском языке как внутри компании, так и за ее пределами.
- Создание отраслевых партнерских отношений между национальными компаниями и иностранными партнерами.
- Создание службы поддержки ИТ-индустрии, чтобы транснациональные компании могли работать из Омана.
- Программа для обеспечения деловой, финансовой и технической поддержки инкубаторов.
- Увеличение отраслевых ассоциаций в создании партнерств.

4. Управление, стандарты и политики

- Разработка и расширение существующих стандартов.
- Переход к большей стандартизации технической архитектуры и инфраструктуры.
- Разработка и принятие соответствующих законов.

5. Инфраструктура нового поколения:

- Совершенствование и активное использование портала e.oman в качестве шлюза для государственных онлайн-сервисов.
- Расширение каналов мобильного доступа к государственным услугам.
- Предложение проводного и беспроводного широкополосного доступа по всей стране по доступной цене.
- Подключение большего числа правительственных сайтов к правительственной сети Омана.
- Использование платформы интеграции услуг для связи и интеграции государственных услуг.
- Использование стандартных общедоступных и масштабируемых строительных блоков государственных служб при создании государственных онлайн-служб.
- Улучшение и расширение унифицированных услуг контактного центра.

6. Продвижение и осведомленность

- Организация целевых кампаний по продвижению и повышению осведомленности об e.oman.
- Проведение просветительских мероприятий HM Award каждые два года.
- Участие в организации отраслевых мероприятий.
- Продвижение глобальных показателей и достижений.

2.2. Рамочная структура архитектуры электронного правительства Омана (OeGAF)

Служит руководством для разработки, развертывания и эксплуатации информационных систем государственных учреждений Омана. OeGAF представляет собой свод стандартов, передовых практик и систем управления процессами для улучшения предоставления государственных услуг в соответствии с миссией Управления информационных технологий (ITA). Она также предназначена для обеспечения основы для управления рисками, связанными с ИТ, объединения средств контроля для их минимизации, более эффективной реализации цифровых инициатив. OeGAF призвана помочь правительству действовать как «интегрированное предприятие» и управлять ИТ как стратегической инвестицией. OeGAF состоит из четырех компонентов[3]: Бизнес-архитектура, Архитектура решения, Информационная архитектура, Техническая архитектура. Каждая из них имеет соответствующую эталонную модель, которая описывает структуру для определения и организации элементов архитектуры.

Ожидаемые бизнес-результаты[4] OeGAF следующие:

а) Более качественные и быстрые государственные услуги гражданам и предприятиям: благодаря стандартизированному доступу к услугам, унифицированным процессам и интегрированной инфраструктуре государственные услуги могут быть улучшены, скоординированы и предоставлены. Важно, чтобы ИТ-стандарты и передовой опыт служили катализатором и основой для интеграции всеми государственными учреждениями своей ИТ-инфраструктуры, приложений и бизнес-процессов, чтобы граждане, резиденты и коммерческие учреждения взаимодействовали с единым правительством Омана.

б) Более эффективное и действенное правительство Омана: принятие и адаптация международных стандартов и передовой практики в области ИТ позволяет улучшить взаимодействие внутри и между различными государственными учреждениями. Улучшение интеграции и сотрудничества между государственными учреждениями приведет к предоставлению более эффективных и действенных государственных услуг.

3 https://www.ita.gov.om/ITAPortal/Pages/Page.aspx?NID=559&PID=1886&LID=98
4 https://www.ita.gov.om/ITAPortal/Pages/Page.aspx?NID=559&PID=1905&LID=99

в) Оптимизация ресурсов и инвестиций: благодаря стандартизации текущие ресурсы и инвестиции могут быть лучше использованы и оптимизированы. Архитектурные стандарты потребуют соответствия и взаимодействия между текущими и новыми инвестициями в ИТ.

2.3. Национальная программа по искусственному интеллекту и передовым технологиям

Программа[5] действует с 2020 года. Министерство транспорта, связи и информационных технологий осуществляет надзор за выполнением следующих задач:

- разработка комплексной национальной программы для искусственного интеллекта (ИИ) и передовых технологий, которая включает политику, законодательство, наращивание потенциала, исследования, инновации, производство, инвестиции и создание стартапов;
- координация и сотрудничество с заинтересованными сторонами из государственного, частного и академического секторов для обмена требованиями, связанными с ИИ и передовыми технологиями, и интеграция с существующими инициативами и проектами;
- координация и связь с местными властями, развитыми странами и международными организациями, связанными с ИИ и передовыми технологиями.

3. Законодательство в сфере информационной безопасности

Общее законодательство в области цифровых технологий затрагивает такие ключевые вопросы, как электронное право, интеллектуальная собственность, налогообложение и защита данных, юридическое признание электронных подписей, допустимость и доказательная сила сообщений данных, осуществление электронных платежей, вопросы юрисдикции, время и место отправки сообщений данных, хранение цифровых сообщений, принудительное исполнение «умных» контрактов, подтверждение получения сообщений и защита конфиденциальности и безопасности.

Оман присоединился к Арабской конвенции о борьбе с преступлениями в области информационных технологий и имплементировал ее положения в национальном законодательстве.

Закон о кибербезопасности в соответствии Королевским указом №12/2011 о киберпреступлениях[6] регулирует юридические действия, которые должны

5 https://www.mtcit.gov.om/ITAPortal/Data/English/DocLibrary/202161395323666/Future%20Opportunities%20for%20Artificial%20Intelligence%20(AI)%20Applications%20in%20the%20Sultanate%20of%20Oman%202.pdf

6 https://omanportal.gov.om/wps/wcm/connect/a42af2b7-ad3f-45aa-9a28-750fd421cd97/Royal+Decree+no+12-2011.pdf?MOD=AJPERES

быть осуществлены в следующих случаях: нарушение безопасности и конфиденциальности данных, электронной информации и информационных систем; злоупотребление средствами информационных технологий; подделки и информационное мошенничество; контентных преступлений; посягательства на кредитные карты. Разработка закона о киберпреступности была основана на Будапештской конвенции, а также на местном, региональном и международном законодательстве, поскольку Султанат считает, что каждый гражданин и житель Омана должен обеспечить полное безопасное использование компьютерных сетей и устройств.

Закон об электронных транзакциях Султаната Оман[7] утвержден Королевским указом Его Величества 69/2008. Это важная веха в реализации Управлением информационных технологий Омана национальной стратегии в области ИТ. Данный закон стал первым нормативным актом о легализации электронных транзакций в Омане, которые определяются как любой контракт, соглашение или сообщение полностью или частично осуществляемые с помощью электронных средств в виде электронных сообщений, и использования для этого открытой криптографии (PKI).

Законопроект о защите персональных данных. В 2017 году объявлено о разработке документа, но пока он остается проектом без четкого указания, когда закон будет принят[8]. Предполагается, что в случае одобрения и подписания закон предоставит широкие права физическим лицам в Омане, схожие с директивой ЕС (GDPR), позволяя им осуществлять контроль над своими личными данными и предоставляя людям право:

- возражать против обработки своих персональных данных;
- требовать доступа к любым личным данным о них, хранящимся в любой организации в Омане;
- требовать исправления любых ошибок в этих данных;
- потребовать, чтобы персональные данные были полностью стерты, если они того пожелают.

Управление информационных технологий проводит консультации с общественностью для обсуждения этого законопроекта и получения отзывов от представителей общественности. В июле 2020 г. Государственный совет провел очередное заседание, на котором обсудил законопроект, отметив его важность в свете текущих технологических разработок и цифровых проблем.

7 https://omanportal.gov.om/wps/wcm/connect/3798ffd0-d1a0-4a41-970f-a5f211f50c3b/Electronic+Transactions+Law+English.pdf?MOD=AJPERES

8 https://www.pwc.com/m1/en/media-centre/articles/oman-latest-developments-data-protection-cybersecurity.html

4. Основные угрозы информационной безопасности и общие подходы к противодействию этим угрозам, в том числе основные направления обеспечения информационной безопасности, включая используемые ключевые институты и инструменты защиты

В контексте борьбы с киберугрозами Оман сосредотачивает внимание на пяти основных направлениях кибербезопасности — правовом, техническом, организационном, наращивании потенциала и сотрудничестве.

Среди основных угроз для информационной безопасности отмечаются кибератаки, «киберзаражения» (в т.ч. программы-вымогатели), кибершантаж.

В Султанате Оман действует ряд государственных политик в сфере развития ИКТ и обеспечения их безопасности[9].

- Политика управления ИТ. Цель этого документа — ввести управление корпоративными ИТ (GEIT) в государственных учреждениях страны.
- Политика управления информационной безопасностью направлена на обеспечение согласованного подхода и установление практики к управлению информационной безопасностью во всех государственных административных единицах.
- Политика открытых государственных данных. Целью этой политики является установление обязательного минимального стандарта безопасности и последовательного подхода к публикации открытых данных, собранных или подготовленных правительством Султаната Оман для достижения целей открытых данных.
- Политика непрерывности предоставления услуг ИКТ для обеспечения общего управления непрерывностью услуг ИКТ в государственных административных единицах, в том числе во время дестабилизирующих событий.
- Политика удаленного доступа к ИКТ. Целью этой политики является определение общего управления предоставлением и использованием удаленного доступа к ресурсам ИКТ в государственных административных единицах.

Под эгидой Министерства транспорта, связи и информационных технологий принята и действует Государственная программа соответствия, цель которой — следить за внедрением всех политик, стандартов и мандатов, выдаваемых государственным административным единицам страны в сфере информационной безопасности.

9 https://www.ita.gov.om/ITAPortal/Pages/Page.aspx?NID=2038&PID=200056

Программа включает в себя элементы:

- оценка: государственным административным единицам предлагается оценить свое соблюдение всех политик, стандартов и других обязательных требований, опубликованных Министерством транспорта, связи и информационных технологий, используя специальные ссылки. При этом в систему могут войти только координаторы и уполномоченные сотрудники государственных административных единиц;
- аудиты соответствия: группа программы соответствия министерства проводит выездные проверки, чтобы убедиться, что государственные административные единицы соблюдают изданные политики, стандарты и рамки;
- отслеживание и отчетность: Министерство несет ответственность в рамках этой Программы за подготовку отчетов о соответствии для уведомления государственных административных единиц о результатах аудитов соответствия и пробелах, если таковые имеются, для принятия корректирующих действий, а также осуществляет регулярные последующие действия. В конце года Кабинету Министров представляется сводный отчет о результатах проверок, дающий представление о состоянии соблюдения государственными административными единицами требований правительства.

Под эгидой Министерства транспорта, связи и информационных технологий разработан собственный стандарт безопасности баз данных (текст доступен только на арабском языке), а также рекомендован к использованию международный стандарт управления рисками информационной безопасности ISO 270001.

В Султанате Оман реализована единая для всех государственных органов информационная инфраструктура на базе облачных сервисов G-Cloud[10], которая призвана обеспечить достижение следующих целей:

- предоставление государственным организациям технологической платформы для размещения их приложений, услуг;
- обеспечение адекватного и оптимального использования вычислительных ресурсов и вспомогательной инфраструктуры подключения (MPLS/Интернет);
- поддержка использования ИТ с открытым программным кодом;
- предоставление всех моделей облачных услуг (IaaS, PaaS, SaaS);
- обеспечение автоматического динамического предоставления ресурсов государственным организациям;
- передача ноу-хау разработки с открытым программным кодом оманским ресурсам.

10 https://www.ita.gov.om/g-cloud/G-Cloud.aspx

Внедрение и управление правительственной сетью передано оманской телекоммуникационной компании (Omantel), которая вложила значительные средства в расширение сети на интернет-протоколе для виртуальных частных сетей.

В целях обеспечения безопасного использования национальных информационных систем и цифровых государственных услуг Министерством транспорта, связи и ИТ разработана инфраструктура открытых ключей (PKI)[11], использование которой утверждено Королевским указом 69/2008. В рамках данной инициативы Султанат внедрил идентификацию для обеспечения целостности, подлинности и конфиденциальности данных, а также личности физических и юридических лиц, получающих к ним доступ. Национальная PKI Омана поддерживает настройку доверенных пространств с использованием функций шифрования, аутентификации и цифровой подписи.

5. Государственные органы, входящие в систему обеспечения информационной безопасности

5.1. Министерство транспорта, связи и информационных технологий

Министерство[12] является головным в Султанате Оман за обеспечение информационной безопасности, разработку и реализацию стратегии электронного правительства. В его обязанности также входит наращивание ориентированных на цифровизацию человеческих ресурсов для обеспечения успешного внедрения государственных электронных услуг. Согласно политике Министерства это ведет к повышению роли граждан в использовании таких цифровых услуг.

Министерство придерживается подхода сокращения государственных расходов, связанных с ИТ, за счет использования консультационных услуг на этапах ИТ-проектов. Для достижения этой цели Министерство реализует стратегические проекты, такие как Единая правительственная сеть Омана, портал государственных электронных услуг, закон об электронных сделках, официальный портал государственных электронных услуг, национальные учебные проекты в области ИТ и информационных систем и др.

Министерство транспорта, связи и информационных технологий берет на себя роль Центрального информационного управления (CIO) государственных электронных услуг. Организационная структура Министерства состоит из управлений и специализированных центров, таких как Главное управление политики и управления, Главное управление инфраструктуры и цифровых платформ, Главное управление стимулирования сектора и будущих навыков, Главное управление цифровой трансформации и расширения возможностей секторов, Национальный

11 https://www.ita.gov.om/ITAPortal/Pages/Page.aspx?NID=965&PID=4109&LID=191
12 https://www.ita.gov.om/ITAPortal/ITA/default.aspx

центр космических и передовых технологий и искусственного интеллекта, национальная группа реагирования на компьютерные инциденты OCERT. Задачи некоторых из них кратко описаны ниже.

5.2 Управление инфраструктуры и цифровых платформ (ITA)[13] отвечает за реализацию национальных проектов в области ИТ-инфраструктуры и надзор за всеми проектами, связанными с реализацией стратегии цифрового Омана. Оно служит в качестве центра компетенций по передовому опыту в области электронного управления и использования ИКТ, а также обеспечивает руководство различными инициативами Султаната в области электронного управления. Отдел информационной безопасности Управления определяет стандарты, политики и процедуры безопасности для Стратегии e.oman.

5.3. Группа готовности к компьютерным чрезвычайным ситуациям Омана (OCERT)

Группа разрабатывает непрерывные процессы мониторинга безопасности, выступая в качестве надежного центра компетенции, знаний и поддержки. OCERT[14] был официально запущен в апреле 2010 г. для анализа рисков и угроз безопасности, которые могут возникнуть в киберпространстве, и доведения этой информации до пользователей. Услуги OCERT ориентированы на пользователей Интернета, правительственные учреждения, частную и критическую национальную инфраструктуру. OCERT разрабатывает технические рекомендации и технические отчеты для администраторов сетей, систем и приложений в государственных и частных учреждениях, а также для частных лиц, чтобы предотвратить их атаки.

OCERT направлен на выполнение следующих задач:

- обеспечить максимально безопасное киберпространство при использования государственных электронных услуг для каждого гражданина и гостей страны;
- поощрять квалифицированных специалистов в области информационной безопасности к работе в различных органах и учреждениях;
- реагировать на любые проблемы с безопасностью и уменьшать их влияние;
- повышать осведомленность о важности кибербезопасности среди оманского общества.

Для этого OCERT предоставляет следующие услуги:

- мониторинг активных сайтов для обнаружения любых угроз или атак;
- проведение обучающих и ознакомительных курсов, сессий и семинаров;

13 https://www.cybersecurityintelligence.com/information-technology-authority-ita-oman-4206.html
14 https://www.cert.gov.om/

- предоставление превентивного и непосредственного реагирования на любой инцидент в режиме реального времени;
- защита или восстановление систем, которые были затронуты компьютерным инцидентом, путем предоставления рекомендаций.

В составе OCERT создана лаборатория для работы с цифровыми доказательствами электронных преступлений и предоставления их суду для осуществления процессуальных действий. Указанная практика нацеливается на получение международного признания, которое повышает доверие к лаборатории и цифровым доказательствам.

OCERT с 2013 года обеспечивает работу Регионального центра кибербезопасности Лиги арабских государств.

5.4. Национальный центр данных в составе Министерства транспорта, связи и информационных технологий создан в сотрудничестве с другими государственными органами. В нем находится централизованный репозиторий важной информации, ИТ-приложений и корпоративных данных.

Задачи Центра:

- обеспечение непрерывности бизнеса, повышение эффективности и снижение расходов правительства;
- улучшение интеграции и масштабируемости приложений в государственных учреждениях;
- обеспечение доступа к безопасным электронным услугам в любое время;
- защита конфиденциальности, целостности, доступности данных граждан и правительства.

В июне 2020 г. султан Омана издал Королевский указ № 64 от 2020 года о создании Центра киберзащиты. В статье 1 Указа говорится, что он будет подчиняться Службе внутренней безопасности Омана. Подзаконные акты и решения, необходимые для внедрения данной системы, будут изданы ее руководителем[15].

6. Участие в международном сотрудничестве в области формирования системы обеспечения международной информационной безопасности в рамках ООН и позиция при голосовании по наиболее важным резолюциям ГА ООН

Оман поддержал все резолюции, разработанные в ходе работы ГПЭ и РГОС. В 2013 году он официально представили свои материалы к докладу ГПЭ, подчеркнув главенствующую роль ООН в решении рассматриваемых группой вопросов.

15 https://www.pwc.com/m1/en/media-centre/articles/oman-latest-developments-data-protection-cybersecurity.html

7. Участие в международном сотрудничестве с другими международными организациями в области формирования системы обеспечения информационной безопасности на региональном уровне

Султанат Оман проводит максимально активную политику сотрудничества по вопросам информационной безопасности на разных уровнях.

7.1. Арабский региональный центр кибербезопасности и (ARCC) [16] создан МСЭ и Султанатом Оман в декабре 2012 г. в лице Министерства технологий, связи и ИТ с целью создать более безопасную и совместную среду в области кибербезопасности в арабском регионе и повысить роль МСЭ в укреплении доверия и безопасности при использовании информационных и коммуникационных технологий в регионе. В соответствии с целями Глобальной программы кибербезопасности МСЭ ARCC служит для локализации и координации инициатив кибербезопасности в арабском регионе и управляется Национальным центром информационной безопасности Омана (OCERT).

- Отвечает за определение требований кибербезопасности арабского мира.
- Играет ключевую роль в глобальной поддержке сетей ITU-IMPACT в различных регионах путем локализации услуг кибербезопасности в соответствии с потребностями арабских стран.
- Организует ежегодные региональные саммиты по кибербезопасности.
- Принимает участие в заседаниях Рабочей группы Совета МСЭ по защите детей в онлайн-среде.

7.2. Учения кибербезопасности. Министерство транспорта, связи и информационных технологий (OCERT и Центр киберзащиты) организует национальные учения по кибербезопасности[17]. Они направлены на повышение готовности к инцидентам путем усиления координации и сотрудничества между OCERT, государственными и частными учреждениями, правоохранительными органами, а также в целях улучшения осведомленности о механизмах и процедурах, используемых для борьбы с киберрисками и угрозами, и подготовки национальных кадров для борьбы с ними. Седьмые по счету учения прошли в октябре 2021 г.[18]

7.3. Оман является членом Альянса кибербезопасности для взаимного прогресса[19] — сетевой платформы для повышения общего уровня кибербезопас-

16 https://arcc.om/
17 https://www.ita.gov.om/ITAPortal/MediaCenter/NewsDetail.aspx?NID=81226
18 https://cert.gov.om/media_news_details.aspx?news=92
19 https://www.cybersec-alliance.org/camp/index.do

ности за счет обмена опытом разработки и тенденциями с участием МСЭ и Организации исламского сотрудничества.

7.4. Соглашение с аналитической компанией Ernst and Young дает возможность Оману участвовать в Глобальном исследовании информационной безопасности (GISS)[20], которое предоставляет организациям и государствам возможность сравнить себя с остальными по важным вопросам информационной безопасности и получить информацию для принятия ключевых решений.

8. Внедрение передовых ИКТ

8.1. Блокчейн

В настоящее время Оман работает над своей первой цифровой валютой. Ранее криптовалюты вызывали беспокойство у властей, в частности, опасения по поводу их использования в мошенничестве. Но с продвижением ИКТ в странах Персидского залива отношение изменилось, в стране технологии блокчейн приветствуются. Dhofar Bank, один из крупнейших банков Омана, уже экспериментировал с технологией, используя технологию RippleNet, чтобы обеспечить более быстрые и дешевые трансграничные платежи в Индию.

8.2 Распространение 5G

Компании Vodafone Oman и Ericsson объявили о развертывании внутренней системы 5G в центре Vodafone Experience Hub в Маскате, а также в офисах головного офиса Vodafone Oman[21]. Все крупные города Султаната покрываются сигналом 5G операторами Omantel, Ooredoo и Vodafone[22].

9. Содержание и оценка предложений и инициатив в области формирования системы обеспечения международной информационной безопасности

В марте 2021 г. Султанатом Оман проведен Всемирный саммит по кибербезопасности, собравший более 300 онлайн-участников, среди которых были высокопоставленные чиновники, директора глобальных компаний информационной безопасности, лидеры в области кибербезопасности[23]. Мероприятие затронуло такие важные темы, как государственная кибербезопасность и стратегии защиты,

20 https://www.itu.int/en/ITU-D/Cybersecurity/Pages/Oman-third-best-prepared-in-world-to-thwart-cyber-attacks.aspx
21 https://developingtelecoms.com/telecom-technology/wireless-networks/13234-vodafone-oman-and-ericsson-take-5g-indoors.html
22 https://www.omantel.om/Personal/AtHome/5G-Home-offer
23 https://www.benzinga.com/pressreleases/21/03/a20376655/the-oman-edition-of-the-world-cyber-security-summit-shed-light-on-mitigating-cyber-threats-and-sec

создание основы кибербезопасности для критически важных активов и критически важной инфраструктуры, нормативно-правовая база, технологии кибербезопасности для умных городов будущего, безопасность цифровых рабочих мест, создание безопасного удаленного рабочего места и др.

17. ПАЛЕСТИНА

Официальное название: Государство Палестина

Столица: Рамалла (де-факто)

Официальный язык: арабский

Территория: 6020 км². В административном отношении Палестина делится на 16 губернаторств. Губернаторы назначаются Президентом и в координации с мэриями и муниципалитетами выполняют в основном административно-хозяйственные функции. Территория Государства Палестина делится на 10 провинций на Западном берегу реки Иордан — Хеврон, Наблус, Рамалла/Эль-Бира, Тулькарм, Дженин, Вифлеем, Тубас, Иерихон, Сальфит и 5 провинций в секторе Газа — Газа, Хан-Юнис, Северная Газа, Рафах, Дейр-эль-Балах, а также провинцию Иерусалим.

Население: 4 816 503 чел. (по оценкам на 2016 год), что является 124-м показателем в мире.

Государственное устройство: Главой Палестины на состоявшихся в январе 2005 г. выборах был избран Махмуд Аббас (Абу Мазен). С 2012 года, после переименования Палестинской национальной администрации в Государство Палестина — Президент Государства Палестина. Президентские выборы не проводились с 2005 года.

Законодательный орган власти — Палестинский законодательный совет (ПЗС). 22 декабря 2018 г. Конституционный суд Палестины принял решение о роспуске ПЗС.

Функции исполнительной власти в соответствии с Основным законом разделены между президентом Палестины и правительством. Однако фактически вся полнота власти сосредоточена в руках М.Аббаса.

Экономика: Показатели ВВП (Паритет покупательной способности) за 2019 год:

- Итого: $30,355 млрд (134-й показатель в мире)
- На душу населения: $6099 (129-й показатель в мире)

Показатели ВВП (Номинал) за 2019 год:

- Итого: $17,051 млрд (125-й показатель в мире)
- На душу населения: $3426 (131-й показатель в мире)

Дипломатические отношения с Россией (СССР): установлены в конце ноября 1974 г.

1. Уровень развития системы обеспечения информационной безопасности и информационно-коммуникационной инфраструктуры (включая индекс развития ИКТ по оценкам МСЭ и ООН)

По данным МСЭ, с 2012 года позиция государства Палестина в глобальном рейтинге снижалась и к 2021 году государство заняло 122-е место, что является ниже среднего показателя среди государств-членов ЛАГ. Несмотря на это уровень проникновения Интернета в стране в настоящее время составляет 64,8%.

Интегральный индекс кибербезопасности Палестины, рассчитанный МСЭ с учетом развития правовой системы обеспечения информационной безопасности, технических и организационных мер, реализации программ наращивания потенциала и участия в международном сотрудничестве, в 2021 году составил всего 25,18 (из 100). Это существенно ниже общемирового показателя.

Власти страны создали Управление для повышения уровня электронного правительства, но достигнутый прогресс не привел к целостному преобразованию, которое должно было повысить уровень жизни граждан и сделать предоставление услуг устойчивым к внешним вызовам.

2. Основные документы стратегического планирования и нормативной базы в области обеспечения информационной безопасности

2.1. Стратегический план для отрасли телекоммуникаций, информационных технологий и почты (2019–2021)

Целями государственной политики, сформулированной в указанном Стратегическом плане[1], были определены следующие:

1) разработка эффективной технической инфраструктуры и современной всеобъемлющей нормативно-правовой базы;
2) построение цифровое общество, способствующее достижению всестороннего и устойчивого развития;
3) доступ к интегрированному электронному правительству;
4) регулирование развитого, всеобъемлющего, конкурентоспособного и эффективного почтового сектора;
5) развитие и укрепление правовой базы, регулирующей сектор связи, ИТ и почту.

В документе приводится анализ сильных и слабых сторон в секторе ИКТ, а также угрозы и возможности. Среди недостатков выделяются: слабость телекоммуникационных услуг для мирового сообщества; скромная доля сектора

1 https://www.mtit.gov.ps/phocadownload/nnn.pdf

в ВВП; слабость и недостатки нормативно-правовой базы; скромные инвестиции и дефицит производства в ИКТ-сфере.

К сильным сторонам причисляются: высокий уровень образования в палестинском сообществе, что обеспечивает государство квалифицированными человеческими ресурсами; заинтересованность правительств в развитии информационного общества; наличие местного капитала для инвестиций в эту сферу; большое участие частного сектора.

2.2. Закон о киберпреступлениях

Первая редакция Закона №16 — 2017[2] была принята в ускоренном режиме без консультаций с экспертным сообществом. Наказания за преступления включают не только лишение свободы и штрафы, но и пожизненное заключение или каторжные работы. Формулировки в законе были расплывчатыми, такими как «угроза безопасности государства, нарушения общественных норм морали, нанесения ущерба национальному единству, гражданских беспорядков и т. д.». Кроме того, закон предоставил Генеральной прокуратуре полномочия проводить обыск лиц по утверждению о нарушении статей закона без предварительного уведомления лица о том, что его электронные сообщения и разговоры отслеживались. Это равносильно серьезному нарушению конфиденциальности пользователей. Статья 20 направлена против распространения новостей, угрожающих «национальному единству», «национальной безопасности» и «общественному порядку».

Чтобы оказать давление на палестинское правительство, коалиции провели встречи между представителями гражданского общества и государственными органами по поводу внесения поправок в Закон 2017 года. Эти продолжающиеся обсуждения в дополнение к кампаниям, начатым активистами, журналистами и юристами, вынудили правительство принять новый закон.

Статья 4 нового закона сохранила свою суть, оставив в силе наказания в виде тюремного заключения и/или штрафа для любого, кто преднамеренно заходит на заблокированные веб-сайты и/или продолжает их использовать, несмотря на то, что осведомлен о блокировке.

Однако, в новом Законе №10 2018[3] также имеются противоречия. В статье 34 второй пункт противоречит первому, а также статье 36. Один пункт статьи разрешает мировому судье отслеживать, записывать, использовать и немедленно юридически возражать против содержания электронных сообщений и разговоров, тогда как другие пункты предоставляют такие полномочия Генеральному прокурору или одному из его помощников.

---

2 https://drive.google.com/file/d/0B0FQQOVEFe9mYm56bWRGT3VkZEE/view?resourcekey=0-AwkN7SoTg_vvpJ0Gn8H2zQ

3 https://security-legislation.ps/sites/default/files/law/Law%20by%20Decree%20No.%2010%20of%202018%20on%20Cybercrime.pdf

Коалиции удалось добиться отмены статьи 20, а также сокращения суровых наказаний, отказа от криминализации, связанной с нечетко определенными терминами, такими как национальное единство и общественный порядок, а также добавления новых положений, таких как статья 21 Закона, который защищает свободу СМИ, публикаций и творчества. Но, несмотря на эти поправки, ряд других проблем, связанных с чрезмерными полномочиями и незаконным сбором доказательств, остались без изменений.

Статья 16 нового закона предусматривает наложение штрафа и/или тюремное заключение того, кто размещает порнографические материалы.

3. Основные угрозы информационной безопасности и общие подходы к противодействию этим угрозам, в том числе основные направления обеспечения информационной безопасности, включая используемые ключевые институты и инструменты защиты

В упомянутом выше Стратегическом плане выделяются следующие угрозы:

а) израильская оккупация и региональная нестабильность;

б) продолжение политического разделения между двумя частями страны;

в) оккупационный контроль над частотами и пограничными переходами;

г) стагнация существующего законодательства, неспособность идти в ногу с развитием сектора и задержка в утверждении законов и нормативных актов, поддерживающих сектор.

Возможностями в документе называются:

а) технический прогресс и появление изобретений, которые могут помочь преодолеть ограничения;

б) политика открытия рынка для иностранных инвестиций, а также участие палестинцев в национальной экономике и передач опыта и знаний;

в) расширение сферы технического образования и создание множества специализированных центров в университетах;

г) заинтересованность государства в проектах отрасли.

3.1. Министерство связи и информационных технологий

Задачи Министерства[4]:

1) определение общей политики и разработка планов и программ развития для секторов телекоммуникаций, почтовой связи и информационных технологий;

2) подготовка, планирование и контроль за реализацией национальной стратегии в области связи и информационных технологий в сотрудничестве и координации с соответствующими органами власти;

4 https://www.mtit.gov.ps/

3) надзор и контроль за секторами телекоммуникаций, почтовых и информационных технологий в Палестине и всеми учреждениями, работающими в них;
4) подготовка необходимых законов и законодательных актов для создания подходящей правовой и законодательной среды для развития сектора телекоммуникаций и информационных технологий;
5) управление, планирование, распределение и контроль национальных частот, лицензирование и регулирование работы радио-, телевизионных, спутниковых и беспроводных передающих станций;
6) создание и управление компьютеризированной и независимой правительственной сетью;
7) обеспечение и развитие почтовых услуг на всех уровнях;
8) лицензирование услуг связи, информационных технологий и почтовых услуг;
9) координация с правительственными учреждениями и другими организациями в отношении сектора связи и информационных технологий;
10) представление Палестины на международных и региональных форумах.

В структуре Министерства действуют несколько ключевых подразделений, занимающихся вопросами информационной безопасности.

Так, одной из задач Главного управления правительственных компьютеров является планирование, контроль и реализация всего, что связано с инфраструктурой информационных технологий, которая включает в себя единую национальную сеть для правительственных учреждений, правительственный центр данных, а также развитие правительственных кадров и местного сообщества в области информационных технологий.

Главное управление информатики работает над разработкой электронных услуг и программного обеспечения с использованием современных технологий и путем подготовки технической инфраструктуры на уровне баз данных, электронных услуг и приложений, что способствует улучшению работы правительства и повышению уровня производительности и прозрачности работы правительства, в дополнение к предоставлению технических консультаций в области информационных технологий для всех учреждений и министерств правительства. Управление также вносит вклад в разработку и успешное выполнение комплексных национальных планов в области информационных технологий и способствует достижению перехода к электронному правительству.

Главное управление электронного правительства контролирует все технические и административные аспекты процесса умной цифровой трансформации на правительственном уровне.

3.2. Палестинская группа реагирования на компьютерные инциденты (PalCERT)

Группа PalCERT реагирует на инциденты компьютерной безопасности и кибербезопасности, предоставляя необходимые услуги для эффективного выявления и координации угроз на правительственном уровне[5].

Задачами группы являются:

1) предоставление доверенного координатора для помощи в защите и реагировании на компьютерные атаки;
2) расширение сотрудничества правительств в области информационной безопасности;
3) содействие совместным исследованиям и разработкам по темам, представляющим интерес для его членов;
4) предоставление материалов и рекомендаций для решения правовых вопросов, связанных с информацией;
5) безопасность и реагирование на чрезвычайные ситуации за пределами государственных границ.

Цель — создать безопасное и надежное киберпространство, используя новейшие технологические инструменты.

4. Участие в международном сотрудничестве в области формирования системы обеспечения международной информационной безопасности в рамках ООН и позиция при голосовании по наиболее важным резолюциям ГА ООН

Государство Палестина не имеет статуса полноправного члена ООН, поскольку не признано тремя государствами-постоянными членами Совета Безопасности ООН (США, Великобританией и Францией).

5. Участие в международном сотрудничестве с другими международными организациями в области формирования системы обеспечения информационной безопасности на региональном уровне

Палестина не сотрудничает с международными организациями.

5 https://www.cert.ps/

6. Содержание и оценка предложений и инициатив в области формирования системы обеспечения международной информационной безопасности

Кибербезопасность Палестины демонстрирует сложные отношения между территориальным суверенитетом и киберпространством. Утверждение суверенитета над национальным киберпространством требует большего, чем контроль над основными сетевыми маршрутами и инфраструктурой.

18. САУДОВСКАЯ АРАВИЯ

Официальное название: Королевство Саудовская Аравия

Столица: Эр-Рияд

Официальный язык: арабский

Территория: 2 149 690 км² (12-я в мире). Саудовская Аравия занимает около 80% территории Аравийского полуострова. На западе страны вдоль берега Красного моря протягивается горная цепь аль-Хиджаз. На юго-западе высота гор достигает 2500 метров. Самая высокая точка Саудовской Аравии — вершина Джабаль-эль-Лауз. Там же расположен курортный район Асир, привлекающий туристов своей зеленью и мягким климатом. Восток же занят в основном пустынями. Юг и юго-восток Саудовской Аравии практически полностью занимает пустыня Руб-эль-Хали, через которую проходит граница с Йеменом и Оманом.

Население: 37 248 169 чел. (по оценкам на 2022 год), что является 40-м показателем в мире.

Государственное устройство: Государственное устройство Саудовской Аравии определяется Основным законом Королевства, носящим название «Основной низам правления Саудовской Аравии», который был принят в 1992 году. Согласно ему Саудовская Аравия является абсолютной теократической монархией, управляемой сыновьями и внуками первого короля Абдул-Азиза. Закон основан на исламском праве. Теоретически власть короля ограничена лишь нормами шариата.

Исполнительная власть в виде Совета министров состоит из премьер-министра, первого заместителя премьер-министра и двадцати министров. Все министерские портфели распределены между родственниками короля и назначаются им самим.

Законодательная власть представлена в виде некоего подобия парламента — Консультативной ассамблеи (Меджлис аш-Шура). Все 150 членов Консультативной ассамблеи назначаются королем на четырехлетний срок. Судебная власть представляет собой систему религиозных судов, где судьи назначаются королем по представлению Верховного судебного совета. Верховный судебный совет в свою очередь состоит из 12 человек, также назначаемых королем. Законом гарантируется независимость суда. Король же выступает в роли высшей судебной инстанции с правом амнистии.

Экономика: Показатели ВВП (Паритет покупательной способности) за 2019 год:

- Итого: $1,677 трлн (17-й показатель в мире)
- На душу населения: $49 216 (23-й показатель в мире)

Показатели ВВП (Номинал) за 2019 год:

- Итого: $792,967 млрд (18-й показатель в мире)
- На душу населения: $23 266 (39-й показатель в мире)

Дипломатические отношения с Россией (СССР): установлены 19 февраля 1926 г.

1. Уровень развития системы обеспечения информационной безопасности и информационно-коммуникационной инфраструктуры

Исходя из статистических данных, уровень развития системы информационной безопасности Саудовской Аравии один из самых высоких в мире:

Индекс МСЭ 2021 кибербезопасности: 99,54 (из 100)

МСЭ 2021, позиция в рейтинге среди ЛАГ: 1

МСЭ 2021, позиция в глобальном рейтинге: 2

МСЭ, уровень проникновения Интернет: 90,1%

NCSI, уровень цифрового развития: 63,46 (из 100)

NCSI, индекс готовности предотвращать киберугрозы и реагировать: 83,12

2. Основные документы стратегического планирования в области обеспечения информационной безопасности

2.1. Национальная Программа «Видение Саудовской Аравии-2030» (Saudi Vision 2030)

Ключевая цель Программы[1] диверсификация экономики королевства, в том числе с помощью цифровой трансформации общества. Руководство страны стремится сделать Саудовскую Аравию одной из ведущих стран мира в области ИКТ, построив цифровую экономику, основанную на принципах четвертой промышленной революции и цифровом управлении обществом. Среди текущих достижений Программы — первое место среди стран G20 в рейтинге «Цифровой рост» по цифровой конкурентоспособности. Целями текущего этапа Программы (2021–2025 годы) являются увеличение вклада цифровой экономики в национальный ВВП до 19,2%, повышение уровня зрелости трансформации основных государственных услуг до 92%.

План цифровизации включает в себя следующие положения:

- развитие прогресса в цифровой среде;
- поддержка инвестиций в телекоммуникации и информационные технологии;
- подготовка и обучение специалистов по кибербезопасности;
- сотрудничество с национальными и международными исследовательскими группами, центрами безопасности, правительственными агентствами;
- обеспечение образовательных и исследовательских целей на национальном и международном уровнях.

1 https://www.vision2030.gov.sa/v2030/vrps/ntp/

2.2. Национальная стратегия кибербезопасности

Стратегия кибербезопасности Саудовской Аравии[2] утверждена в декабре 2020 г. Ее цель — отразить стратегические подходы страны, обеспечивающие баланс между безопасностью, доверием и ростом. Для укрепления Стратегии она устанавливает четыре национальных механизма кибербезопасности:

- национальная система управления киберрисками;
- национальная система реагирования на киберинциденты;
- национальная система по обмену информацией;
- национальная система по наращиванию киберпотенциала.

Стратегия ставит 6 основных целей:

1. комплексное управление кибербезопасностью на национальном уровне
2. эффективное национальное управление киберрисками;
3. защита киберпространства;
4. укрепление национальных технических возможностей по защите от киберугроз;
5. укрепление партнерских отношений и сотрудничество в области кибербезопасности;
6. наращивание национального кадрового потенциала и развитие индустрии кибербезопасности в Королевстве.

2.3. Стратегия цифрового развития Саудовской Аравии на 2019–2023 гг.

Основные приоритеты Стратегии в сфере ИКТ:

- развитие инфраструктуры телекоммуникаций и информационных технологий, особенно высокоскоростного широкополосного доступа;
- разработка техническихх стандартов для облегчения расширения широкополосных сетей;
- создание эффективных партнерств с частным сектором;
- поддержка местных инвестиций в секторах телекоммуникаций и информационных технологий;
- создание «умного» правительства;
- управление цифровым преобразованием.

Основными задачами Стратегии являются: привлечение ведущих международных компаний в приоритетных областях передовых технологий, увеличение доли местного контента в секторе ИКТ, улучшение технических навыков местных специалистов, расширение технических и цифровых знаний, стимулирование технических инноваций путем поощрения исследований и разработок в новой экосистеме Королевства, развитие мегапроектов, а также поддержка ко-

2 https://nca.gov.sa/files/national_cybersecurity_strategy-ar.pdf
https://www.nca.gov.sa/files/national_cybersecurity_strategy-en.pdf

ординации и взаимодействия между соответствующими субъектами ИКТ в государственном и частном секторах.

Достижение целей Стратегии определяется следующими показателями:

- рост ИТ-сектора на 50%;
- увеличение за 5 лет вклада сектора ИКТ в ВВП на 50 млрд саудовских реалов;
- поддержка усилий по локализации технологий путем повышения саудизации рабочей силы до 50% к 2023 году;
- привлечение иностранных инвестиций;
- поддержка расширения прав и возможностей и участия женщин.

3. Законодательство в сфере информационной безопасности

Закон о борьбе с киберпреступностью принят 26 марта 2007 г. Он устанавливает ответственность за нарушения в области распространения информации с целью повышения информационной безопасности, защиты прав, относящихся к законному использованию компьютерных и информационно-телекоммуникационных сетей.

В законе[3] кодифицированы следующие виды компьютерных преступлений:

- перехват или прием данных, передаваемых через информационную сеть или компьютер;
- незаконный доступ к компьютеру с целью шантажа;
- незаконный доступ к сайту или взлом сайта с намерением уничтожить или изменить его, занять его URL-адрес;
- незаконный доступ к банковским данным;
- незаконный доступ к компьютеру с целью уничтожения, утечки, повреждения, изменения или распространения личных данных;
- изготовление, публикация и распространение материалов порнографического характера;
- создание или распространение информации о сайте, созданном в целях обеспечения возможности торговли людьми;
- создание или распространение информации о сайте, созданном в целях распространения наркотических и иных психотропных веществ;
- создание или распространение информации о деятельности террористических организаций с целью упрощения коммуникации между членами таких организаций, финансирования таких организаций, продвижения их идеологий, публикации методов создания взрывчатых устройств и др.

3 https://laws.boe.gov.sa/BoeLaws/Laws/LawDetails/25df73d6-0f49-4dc5-b010-a9a700f2ec1d/1

Нормативно-правовая база облачных вычислений[4] действует с марта 2019 г., регулирует права и обязанности поставщиков облачных услуг (CSPs), государственных и частных предприятий. Является одним из немногих примеров нормативно-правового регулирования облачных технологий во всем мире. С точки зрения защиты данных, база устанавливает требования к обеспечению безопасности данных для поставщиков облачных услуг. Облачная клиентская информация может квалифицироваться по 4-м уровням безопасности данных, среди которых выделяются:

уровень 1 — отсутствует конфиденциальная информация о физических лицах или о компаниях частного сектора;

уровень 2 — конфиденциальные данные физических лиц, компаний частного сектора, не подпадающие под ограничения на передачу данных;

уровень 3 — конфиденциальные данные физических лиц, компаний частного сектора, подпадающие под ограничения на передачу данных;

уровень 4 — повышенный уровень секретности конфиденциальных данных, принадлежащих государственным органам.

Нормативно-правовая база Интернета вещей — действует с сентября 2019 г.[5] Данное законодательство обязывает лицензированных поставщиков услуг Интернета вещей и внутренних разработчиков сетей Интернета вещей размещать все серверы, используемые для предоставления услуг Интернета вещей, и хранить все данные на территории Саудовской Аравии, а также соблюдать другие законы, правила и требования Комиссии по коммуникационным и информационным технологиям (CITC) или других органов (все существующие и принятые в будущем), касающиеся управления данными, конфиденциальности и защиты данных. Поставщики услуг Интернета вещей обязаны хранить данные в течение 12 месяцев.

В Саудовской Аравии отсутствует общегосударственное законодательство по защите персональных данных, однако действует ряд корпоративных стандартов защиты данных, признаваемых в качестве «образцовых»: Saudi Arabian Airlines (Saudia) [6], SABIC[7], Saudi Aramco[8].

4 Полный текст документа доступен по ссылке: https://www.citc.gov.sa/en/RulesandSystems/RegulatoryDocuments/Documents/CCRF_En.pdf

5 Материалы доступны по ссылке: https://www.citc.gov.sa/en/RulesandSystems/RegulatoryDocuments/Documents/IoT_REGULATORY_FRAMEWORK.pdf

6 https://www.saudia.com/help/useful-links/legal-and-terms-and-conditions/data-protection-policy

7 https://www.sabic.com/en/data-protection

8 https://www.aramco.com/en/website-information/privacy-statement#

4. Основные угрозы информационной безопасности и общие подходы к противодействию этим угрозам, в том числе основные направления обеспечения информационной безопасности, включая используемые ключевые институты и инструменты защиты

Национальное управление по кибербезопасности Саудовской Аравии выделило следующие угрозы:

1. несанкционированная деятельность
2. вредоносные коды;
3. попытки эксплуатации;
4. утечка информации;
5. подделка доменного имени.

5. Государственные органы, входящие в систему обеспечения информационной безопасности

5.1. Министерство связи и информационных технологий

Министерство[9] осуществляет надзор за сектором связи и информационных технологий и связанной с ним деятельностью; разрабатывает политику, регулирующую сектор ИКТ и планы деятельности в сфере ИКТ.

Под контролем Министерства находятся три национальные программы:

- обеспечение развития платформ для цифрового общества, цифровой экономики и цифровой страны;
- yesser: Программа электронного правительства, направленная на повышение производительности и эффективности государственного сектора путем предоставления необходимых услуг и информации;
- функционирование Национального центра цифровой сертификации[10] и управление инфраструктурой открытых ключей для обеспечения безопасной, эффективной передачи и обмена информацией в электронной форме между ключевыми заинтересованными сторонами, включая правительство, граждан и бизнес-сектор.

5.2. Комиссия по связи и информационным технологиям

Комиссия[11] является национальной администрацией связи и осуществляет свою деятельность с целью развития сектора связи и информационных технологий, создания высококонкурентной среды, предоставления услуг связи, создания привлекательной экосистемы для инвесторов. В ее функции входит:

9 https://www.mcit.gov.sa/
10 https://www.mcit.gov.sa/en/program/ncdc
11 https://www.citc.gov.sa/en/Pages/default.aspx#?

- регулирование сектора связи и информационных технологий;
- отслеживание и внедрение разработок в области технологий и услуг сектора связи и информационных технологий;
- развитие условий для инвестиций в секторе коммуникаций и информационных технологий в Королевстве.

Под эгидой Комиссии регулярно проводятся обучающие / тренировочные кампании по информационной безопасности с целью защиты прав пользователей ИКТ, а также разрабатывается необходимая нормативная база.

5.3. Национальное управление по кибербезопасности

Управление[12] выполняет как регулирующие, так и операционные функции, связанные с кибербезопасностью, и тесно сотрудничает с государственными и частными организациями для улучшения состояния кибербезопасности страны, чтобы защитить ее жизненно важные интересы, национальную безопасность, критически важные инфраструктуры, высокоприоритетные сектора и государственные услуги. Деятельность ведется в соответствии с Saudi Vision 2030.

Национальное Управление имеет всеобъемлющий мандат, который включает разработку национальной стратегии кибербезопасности и надзор за ее реализацией; разработку системы кибербезопасности, средств контроля и соблюдение нормативных требований; создание и эксплуатацию операционных центров кибербезопасности; развитие кадрового потенциала в области кибербезопасности; повышение осведомленности; стимулирование роста сектора кибербезопасности и поощрение инноваций и инвестиций в него; установление связей с аналогичными агентствами за рубежом и частными организациями для взаимного обмена знаниями и опытом в области кибербезопасности.

5.4. Управление по Большим данным и искусственному интеллекту

Управление[13] ориентировано на использование технологий Больших данных и программы развития искусственного интеллекта, включает в себя несколько вспомогательных органов, таких как Национальный центр в области развития искусственного интеллекта (NCAI), Национальный центр информации (NIC), Отдел управления данными (NDMO).

5.5. Центр реагирования на компьютерные инциденты CERT-SA

Центр[14] действует с 2006 года, является некоммерческой структурой, предназначенной для повышения и развития уровня осведомленности, знаний, управ-

12 https://www.nca.gov.sa/en/index.html
13 https://sdaia.gov.sa/
14 http://cert.sa/index_en.html

ления, обнаружения, предотвращения, координации и реагирования на случаи информационной безопасности на национальном уровне. Данный центр подчиняется Комиссии по связи и информационным технологиям.

Саудовская Федерация кибербезопасности и программирования — национальное учреждение[15], действует под эгидой Олимпийского комитета Саудовской Аравии, стремится наращивать национальный и профессиональный потенциал в области кибербезопасности и программирования в соответствии с признанными международными практиками и стандартами, чтобы ускорить восхождение страны в ряды развитых стран в области технологических инноваций. В рамках достижения указанных целей Федерация занимается проведением конференций, повышением осведомленности общественности о важности кибербезопасности и программирования, поддержкой молодых талантов; проведением образовательных программ, оказанием помощи в восстановлении и развитии самобытных национальных компетенций; проведением соревнований, поддержкой участия молодых талантов в местных или международных соревнованиях по кибербезопасности и программированию. В 2019 году Федерация организовала образовательную программу «Тувайкский киберкамп» — самое большое мероприятие подобного рода на Ближнем Востоке.

Центр передового опыта в области информационного обеспечения (CoEIA[16]) в Университете King Saud является некоммерческой структурой, целью которой является разработка и предоставление решений в области безопасности для повышения уровня информационной безопасности как в государственном, так и в частном секторах. Центр также предоставляет консультационные услуги по безопасности компьютерных сетей и информационных систем, применению международных стандартов, а также по разработке учебных и учебных программ, специализирующихся в области информационной безопасности, в соответствии с потребностями учреждений и организаций, работающих в различных областях. Тесно сотрудничает с большим количеством известных учреждений и исследовательских центров по всему миру в области информационной безопасности.

6. Участие в международном сотрудничестве в области формирования системы обеспечения международной информационной безопасности в рамках ООН и позиция при голосовании по наиболее важным резолюциям ГА ООН

Непосредственного участия в работе ГПЭ Саудовская Аравия не принимала, но голосовала за разработанные ею рекомендации.

15 https://safcsp.org.sa/en/
16 https://coeia.ksu.edu.sa/en/about

7. Участие в международном сотрудничестве с другими международными организациями в области формирования системы обеспечения информационной безопасности на региональном уровне

В октябре 2017 г. состоялось подписание Меморандума о взаимопонимании между Министерством связи и массовых коммуникаций Российской Федерации и Министерством связи и информационных технологий Королевства Саудовская Аравия о сотрудничестве в области связи и информационно-коммуникационных технологий.

Меморандум закрепил обоюдное намерение партнеров вести совместную работу по целому перечню направлений сферы ИКТ, которые затрагивают не только отдельные вопросы развития сферы связи и информационных технологий, но и глобальные направления сотрудничества. Так, положениями меморандума предусматривается усиление сотрудничества в области широкополосного доступа в сеть Интернет, управления сетью Интернет, электронного правительства, совместную разработку программного обеспечения, цифрового контента, облачных вычислений, больших данных, «интернета вещей». В рамках меморандума стороны осуществляют сотрудничество в области подготовки кадров в сфере связи и ИКТ, а также содействуют отраслевому сотрудничеству и инвестициям, совместным инновациям, проведению исследований, обмену технологиями в профильных областях.

В 2019 году Россия и Саудовская Аравия подписали Исполнительную программу технологического сотрудничества и Меморандум о сотрудничестве в области массовых коммуникаций. В рамках соглашений стороны договорились развивать совместные проекты в сферах искусственного интеллекта и «умного» города. Тогда же подведомственный Минцифры России фонд «Росинфокоминвест» подписал Меморандум о взаимопонимании с Saudi Business Machines (официальный представитель IBM World Trade Corporation в королевстве). Документ подразумевал реализацию маркетинговых и образовательных проектов по темам кибербезопасности, обработки и анализа больших данных и искусственного интеллекта.

В 2018 году Саудовская Федерация кибербезопасности и программирования подписала три Меморандума о взаимопонимании с США о сотрудничестве с американскими компаниями, обслуживающими ВПК США — Lockheed Martin, Raytheon Company, Northrop Grumman.

В конце 2020 года Национальное Управление кибербезопасности в сотрудничестве с МСЭ подписало Соглашение о стратегическом партнерстве по запуску глобальной программы безопасного и процветающего киберпространства для детей.

8. Содержание и оценка предложений и инициатив в области формирования системы обеспечения международной информационной безопасности

Предложений Саудовской Аравии по данному направлению деятельности не выявлено.

19. СИРИЯ

Официальное название: Сирийская Арабская Республика

Столица: Дамаск

Официальный язык: арабский

Территория: 185 180 км² (87-я в мире). Территория подразделяется на западную прибрежную зону, опоясанную узким двойным горным хребтом, и более обширную зону на востоке, представляющую собой плато. Самым главным природным ресурсом страны является плодородная почва, предпринимались множественные попытки увеличения обрабатываемых площадей путем орошения. Вдоль Средиземного моря протянулась узкая прибрежная равнина от Турции до Ливана. Поверхность этой литоральной зоны покрыта песчаными дюнами, которые лишь изредка прерываются холмами, спускающимися от гор к морю. Сирия претендует на территориальные воды Средиземного моря на расстоянии 35 морских миль (65 км) от берега.

Население: 17 070 000 чел. (по оценкам на 2019 год), что является 71-м показателем в мире.

Государственное устройство: Сирия — многопартийная президентско-парламентская республика.

Глава государства — президент. Президент согласно конституции страны избирается на 7 лет, количество сроков пребывания у власти ограничено двумя сроками подряд. Президент имеет право назначать кабинет министров, объявлять военное или чрезвычайное положение, подписывать законы, объявлять амнистию, а также производить поправки к конституции. Президент определяет внешнюю политику страны и является верховным главнокомандующим вооруженных сил.

Законодательная власть в стране представлена Народным советом. Депутаты 250-местного парламента избираются прямым голосованием на четырехлетний срок. Народный совет утверждает бюджет страны, а также занимается законодательной деятельностью.

Судебная система представляет собой уникальное сочетание исламских, османских и французских традиций. Основой законодательства Сирии является, согласно конституции, исламское право, хотя фактически действующее законодательство базируется на Кодексе Наполеона. Существуют три уровня судов:

Суд первой инстанции, Апелляционный суд и Конституционный суд, являющийся высшей инстанцией. Конституционный суд состоит из пяти судей, одним из которых является президент Сирии, а четыре других назначаются президентом. Таким образом в руках президента сосредоточен полный контроль как за исполнительной, так и за законодательной и судебной властью.

Экономика: Показатели ВВП 2010 год:

- Итого: $59,957 млрд
- На душу населения: $2802

Дипломатические отношения с Россией (СССР): установлены 21 июля 1944 г.

1. Уровень развития системы обеспечения информационной безопасности и информационно-коммуникационной инфраструктуры (включая индекс развития ИКТ по оценкам МСЭ и ООН)

По данным МСЭ на 2021 год, Сирия является низкоинформатизированной страной, уровень проникновения Интернета в настоящее время составляет 46,5%. Интегральный индекс готовности к киберугрозам и реагированию на них составляет всего 15,58, уровень цифрового развития равен 33,4 в соответствии с данными NCSI. В глобальном рейтинге кибербезопасности Сирия занимает 126-ю позицию и 16-ю позицию в ЛАГ.

Исходя из перечисленных ниже статистических данных, уровень развития системы информационной безопасности Сирии может быть оценен как очень низкий.

2. Основные документы стратегического планирования в области обеспечения информационной безопасности

В открытом доступе информация по данной теме не обнаружена

3. Основные угрозы информационной безопасности и общие подходы к противодействию этим угрозам, в том числе основные направления обеспечения информационной безопасности, включая используемые ключевые институты и инструменты защиты

В открытом доступе информация по данной теме не обнаружена

4. Участие в международном сотрудничестве в области формирования системы обеспечения международной информационной безопасности в рамках ООН и позиция при голосовании по наиболее важным резолюциям ГА ООН

Сирия активно поддерживает российские инициативы в области международной информационной безопасности, всегда выступая в их поддержку.

В 2018–2020 годах являлась соавтором российских проектов резолюций Генеральной Ассамблеи ООН:

A/RES/73/27 от 5 декабря 2018 г. (принятие правил, норм и принципов ответственного поведения, а также создание Рабочей группы ООН открытого состава);

A/RES/73/187 от 17 декабря 2018 г. (включение в повестку дня ООН обсуждения вопроса о противодействии использованию ИКТ в преступных целях);

A/RES/74/247 от 27 декабря 2019 г. (создание специального межправительственного комитета экспертов открытого состава для разработки всеобъемлющей международной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях);

A/RES/75/240 от 31 декабря 2020 г. (создание новой Рабочей группы ООН открытого состава по вопросам безопасности в сфере использования ИКТ и самих ИКТ 2021–2025).

Проголосовала против принятия американского проекта резолюции Генеральной Ассамблеи ООН A/RES/73/266 от 22 декабря 2018 г. (о создании Группы правительственных экспертов ООН на 2019–2021 годы).

5. Участие в международном сотрудничестве с другими международными организациями в области формирования системы обеспечения информационной безопасности на региональном уровне

Сирия взаимодействует на глобальном и региональном уровнях по вопросам обеспечения кибербезопасности в рамках следующих международных организаций, членом которых он является:

ООН;

ITU (МСЭ);

Движение неприсоединения;

ЛАГ;

Интерпол;

ISO (Международная организация по стандартизации).

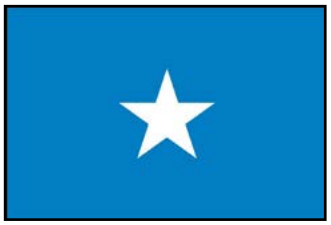
6. Содержание и оценка предложений и инициатив в области формирования системы обеспечения международной информационной безопасности

Сирия:

не присоединилась к инициативе Франции — Парижский призыв к доверию и безопасности в киберпространстве (2018 год);

не стала соавтором инициативы Франции и Египта — Программа действий ООН по продвижению ответственного поведения государств в киберпространстве (2020 год).

20. СОМАЛИ



Официальное название: Федеративная Республика Сомали

Столица: Могадишо

Официальные языки: сомалийский и арабский

Территория: 637 657 км² (41-я в мире). Рельеф страны преимущественно равнинный. На севере и в междуречье Джубы и Веби-Шебели преобладают плато высотой 500–1500 м, сложенные в основном песчаниками и известняками. В понижениях на плато — «баллехах» — скапливается дождевая вода, с давних времен они служат источниками питьевой воды. Плато разделены неглубокими, широкими долинами (Ногаль, Дарор и другие), по которым идут дороги и караванные пути, связывающие внутренние районы с побережьем.

Северный край плато рассечен глубокими ущельями. Там возвышаются горы Уарсанжели-Миджуртина (высшая точка — 2406 м, гора Суруд-Ад). На севере и юго-востоке плато Сомали окаймлены низменностями. Из-за сухого климата и большой водонепроницаемости пород плато безводны, что препятствует развитию земледелия и возникновению постоянных поселений. С давних времен это область преимущественно кочевого скотоводства.

Население: 15 443 000 чел. (по оценкам на 2019 год), что является 73-м показателем в мире.

Государственное устройство: Сомали — федеративная республика, состоящая из пяти федеративных регионов, а также самопровозглашенного государства Сомалиленд. Де-факто, север Сомали разделен между автономным регионом Пунтленд (который рассматривает себя как автономное государство) и Сомалилендом. В центральном Сомали, Галмудуг — другая региональная единица, находящаяся к югу от Пунтленда.

Федеральный Парламент Сомали отвечает за выбор количества и границ автономных региональных (официально — федеральных) государств в составе Федеративной Республики Сомали. С этой целью законодательный орган в декабре 2014 г. принял закон о создании комиссии по границам и федерализации. Этот орган уполномочен определять границы входящих в состав страны федеральных государств, а также проводить арбитражные разбирательства между ними по вопросам их соответствующей юрисдикции.

Экономика: Показатели ВВП (Паритет покупательной способности) за 2019 год:

- Итого: $13,953 млрд (151-й показатель в мире)

Показатели ВВП (Номинал) за 2019 год:

- Итого: $4,942 млрд (148-й показатель в мире)

Дипломатические отношения с Россией (СССР): установлены 11 сентября 1960 г.

1. Уровень развития системы обеспечения информационной безопасности и информационно-коммуникационной инфраструктуры

Исходя из статистических данных, уровень развития системы информационной безопасности Сомали крайне низкий:

МСЭ 2021, индекс кибербезопасности: 17,25 (из 100)

МСЭ 2021, позиция в рейтинге среди государств-членов ЛАГ: 19

МСЭ 2021, позиция в глобальном рейтинге: 137

МСЭ, уровень проникновения Интернет: 12,8%

2. Основные документы стратегического планирования в области обеспечения информационной безопасности

2.1. Национальная политика и стратегия в сфере ИКТ, 2019–2024 годы.

Министерство планирования разработало документ[1], который заменил аналогичный план на 2017–2019 годы. Признано, что существует множество ключевых вопросов, которые необходимо решить для создания оптимальной экосистемы ИКТ, способной содействовать прогрессу в достижении целей устойчивого развития по обеспечению связи и других задач. Например, ограниченный уровень цифровой грамотности, отсутствие местного контента, вопросы безопасности, гендерное неравенство и отсутствие доступного энергоснабжения — все это значительные препятствия, которые необходимо устранить. Данная политика также признает необходимость учитывать быстрое развитие технологий в сфере ИКТ, таких как Интернет вещей (IoT), искусственный интеллект, робототехника и сервисы межмашинного взаимодействия (M2M), сетевой нейтралитет, Большие данные, технологии блокчейн и криптовалюты.

Концепция политики и стратегии в области ИКТ заключается в следующем: использовать потенциальные преимущества ИКТ для поддержки экономического развития и социальной интеграции для всех сомалийцев.

Основная цель политики и стратегии в области ИКТ — обеспечить гражданам Сомали возможность в полной мере воспользоваться огромным потенциалом ИКТ для ускорения развития, создания новых богатств и рабочих мест. Для достижения этой цели и реализации видения данной политики был определен ряд политических задач, охватывающих такие подсектора, как телекоммуникации, радиовещание, почтовые услуги, электронные платежи и системы управления информацией, а также другие межсекторные и новые области.

Ключевые приоритеты для сектора ИКТ в Сомали определяются задачами развития, изложенными в Национальном плане развития (НПР), а также с уче-

1 https://mptt.gov.so/en/wp-content/uploads/2019/11/National-ICT-Policy-Strategy-2019-2024.pdf

том региональных и международных целей, в частности, Целей устойчивого развития (ЦУР) и правительственной стратегии «Создание энергичного, сильного и конкурентоспособного частного сектора, способствующего устойчивому экономическому развитию Федерального правительства Сомали». Исходя из этого, ниже перечислены приоритетные направления деятельности, которые должны быть завершены к 2024 году в рамках данной политики:

- расширение национальной магистральной инфраструктуры для подключения всех крупных городских центров с резервированием/дублированием каналов связи (для обеспечения надежности), а также решение проблем «последней мили» для обеспечения всеобщего доступа к широкополосной связи, включая эффективное межсетевое соединение и расширение зоны покрытия мобильной связи 3/4G;
- создание правительственного центра обработки данных с резервными облачными мощностями;
- обеспечение защиты критической инфраструктуры — создание группы по кибербезопасности и конфиденциальности для надзора за разработкой и внедрением национальной политики кибербезопасности, а также создание группы реагирования на компьютерные чрезвычайные ситуации (CERT);
- обеспечение того, чтобы все законы отражали потребности в продвижении электронной коммерции, обеспечении конфиденциальности данных в Интернете, защиты детей и допустимости электронных доказательств в суде.

2.2. Закон о телекоммуникациях, 2017 год

После принятия в 2017 году Национального закона о коммуникациях Национальное управление связи было создано в качестве регулирующего органа для защиты сектора связи в Сомали. Регулятор осуществляет разработку ряда нормативных актов и единой системы лицензирования. На данный момент за счет лицензирования радиочастотного спектра государство получает с компаний доход в бюджет.

3. Основные угрозы информационной безопасности и общие подходы к противодействию этим угрозам, в том числе основные направления обеспечения информационной безопасности, включая используемые ключевые институты и инструменты защиты

3.1. Министерство почты, телекоммуникаций и технологий

Министерство[2] определяет политическую повестку дня ИКТ-сектора, координируя работу с другими государственными учреждениями, частным сектором,

2 https://mptt.gov.so/

организациями гражданского общества и другими заинтересованными сторонами, консультируя общественность при разработке политики и стратегий сектора. Оно обеспечивает прозрачное, независимое и эффективное регулирование и консультирует Федеральное правительство Сомали по вопросам ИКТ, а также представляет правительство по вопросам политики в области ИКТ на международных конференциях. В его функции также входит координация со Стратегическим планом развития инфраструктуры страны, для чего целевая группа при необходимости может привлекать внешних экспертов.

3.2. Национальное управление связи Сомали (NCA)

Управление[3] является регулирующим органом сектора ИКТ. Созданное в соответствии с Законом о телекоммуникациях 2017 года, оно несет основную ответственность за реализацию политики федерального правительства в этом секторе. Оно обязано разрабатывать постановления, распоряжения, руководства и правила для регулирования сектора при реализации национальной политики в области ИКТ. Закон о связи не содержит прямого упоминания о регулировании почтового сектора, поэтому, в почтовом секторе нет регулирующего органа.

3.3. Сомалийская группа реагирования на компьютерные инциденты/ Координационный центр (SomCERT/CC)

В мае 2019 г. SomCERT/CC[4] был сформирован в качестве подразделения Департамента кибербезопасности Национального управления связи (NCA) с целью обеспечения безопасности киберпространства Сомали и предоставления официального контактного центра для обработки инцидентов кибербезопасности в сомалийском интернет-сообществе.

Миссия Центра — повысить безопасность киберпространства Сомали посредством проактивного предупреждения и эффективных действий, а также повышения осведомленности о кибербезопасности. Также задачи Центра — определять, оценивать, анализировать, разрабатывать и предоставлять ответные меры и решения для Интернет сообщества.

SomCERT/CC обеспечивает обработку инцидентов кибербезопасности, способствует повышению осведомленности о кибербезопасности, а также координирует вопросы кибербезопасности. SomCERT/CC сотрудничает с государственными учреждениями, организациями, научными кругами, поставщиками интернет-услуг (ISP) и другими соответствующими структурами для урегулирования инцидентов кибербезопасности в Сомали и различных инициатив в области кибербезопасности по всему миру, а также обеспечивает своевременное

3 https://nca.gov.so/
4 https://somcert.gov.so/

предупреждение, поддержку и консультации для всех заинтересованных сторон из государственного и частного секторов в предотвращении и урегулировании инцидентов кибербезопасности.

4. Участие в международном сотрудничестве в области формирования системы обеспечения международной информационной безопасности в рамках ООН и позиция при голосовании по наиболее важным резолюциям ГА ООН

Сомали не участвовала в голосовании по российскому проекту резолюции Генеральной Ассамблеи ООН от 5 декабря 2018 г. о переформатировании дискуссии по МИБ в прозрачный, инклюзивный диалог и созыве РГОС.

Резолюция Генеральной Ассамблеи ООН A/RES/73/187 «Противодействие использованию информационно-коммуникационных технологий в преступных целях» от 17 декабря 2018 г. была поддержана.

Сомали одобрила американский проект резолюции Генеральной Ассамблеи ООН «Поощрение ответственного поведения государств в киберпространстве в контексте международной безопасности» (A/RES/73/266 от 22 декабря 2018 г.).

5. Участие в международном сотрудничестве с другими международными организациями в области формирования системы обеспечения информационной безопасности на региональном уровне

5.1. Сотрудничество SomCERT/CC

SomCERT/CC является полноправным и активным членом Организации исламского сотрудничества - Группы реагирования на компьютерные чрезвычайные ситуации (OIC-CERT). SomCERT/CC тесно сотрудничает с Арабским региональным центром кибербезопасности (ARCC), AfricaCERT и МСЭ.

5.2 Модель зрелости потенциала в области кибербезопасности

Сомали сотрудничает с Глобальным центром создания потенциала в области кибербезопасности (GCSCC), Всемирным банком и Норвежским институтом международных отношений, чтобы разработать основу для анализа зрелости потенциала кибербезопасности[5] в стране, улучшить ее состояние в области кибербезопасности.

5 https://cybilportal.org/projects/cmm-review-somalia/

6. Содержание и оценка предложений и инициатив в области формирования системы обеспечения международной информационной безопасности

Государство занято формированием основ кибербезопасности (и даже декларирует готовность принимать у себя киберучения региональных CERT). Правительство не особо спешит официально очерчивать круг задач в киберпространстве, рассчитывая сохранять как можно дольше универсальность системы.

21. СУДАН

Официальное название: Республика Судан

Столица: Хартум

Официальные языки: арабский и английский

Территория: 1 886 068 км² (15-я в мире). Большую часть территории Судана занимает плато (высоты 300—1000 метров), которое с юга на север пересекает долина реки Нил, образуемой слиянием Белого и Голубого Нила. В районе слияния находится столица страны город Хартум. Все реки относятся к бассейну Нила.

На севере страны — Ливийская и Нубийская пустыни, почти лишенные растительности. В центре и на юге страны — саванны и редколесья. На востоке и западе — горы.

Население: 47 460 150 чел. (по оценкам на 2023 год), что является 31-м показателем в мире.

Государственное устройство: Форма государственного правления — республика. Действует временная конституция 2005 года. Глава государства — президент, а правительство с 2017 года вновь возглавляет премьер-министр.

Парламент двухпалатный — Совет провинций (50 мест, избирается органами управления провинций на шестилетний срок) и Национальная ассамблея (450 мест, в 2005 году были назначены президентом — заполнено 360 мест: 355 от президентской партии Национальный конгресс и 5 беспартийных).

С 2020 года у власти находится Переходный временный военный совет. По договоренности между военным руководством страны и гражданским обществом, в 2023 году должен быть избран гражданский премьер-министр, после чего вводится двухлетний переходный период, который завершится всеобщими выборами.

Экономика: Показатели ВВП (Паритет покупательной способности) за 2019 год:

- Итого: $178,950 млрд (72-й показатель в мире)
- На душу населения: $4140 (147-й показатель в мире)

Показатели ВВП (Номинал) за 2019 год:

- Итого: $33,359 млрд (96-й показатель в мире)
- На душу населения: $772 (173-й показатель в мире)

Дипломатические отношения с Россией (СССР): установлены 5 января 1956 г.

1. Уровень развития системы обеспечения информационной безопасности и информационно-коммуникационной инфраструктуры

По данным МСЭ, позиция Судана в глобальном рейтинге с 2002 года снижалась, однако к 2021 году государство заняло 102-е место, что является лучшим для него показателем. Страна остается низкоинформатизированной, уровень проникновения Интернета в настоящее время составляет 29,2%. Соответственно, интегральный индекс кибербезопасности Судана, рассчитанный МСЭ с учетом развития правовой системы обеспечения информационной безопасности, технических и организационных мер, реализации программ наращивания потенциала и участия в международном сотрудничестве, в 2021 году составил всего 35,03 (из 100). Это существенно ниже общемирового показателя. Уровень развития электронного правительства в Судане находится на среднем уровне, тем не менее индекс электронного участия значительно ниже общемирового[1].

2. Основные документы стратегического планирования в области обеспечения информационной безопасности

Стратегическое планирование в Судане имеет свои особенности. Весь комплекс развития государственной политики формулируется на долгосрочную перспективу. Так в 2007 году была принята 25-летняя Национальная стратегия (2007–2030), конкретизация которой осуществляется путем разработки пятилетних или тематических планов. В частности, при поддержке Республики Корея был сформирован Мастер-план развития электронного правительства и трансформации его в «умное» правительство (2016–2020).

Однако стратегическое планирование в сфере информатизации и обеспечения информационной безопасности фрагментарное. В 1999 году была принята Национальная стратегия развития ИКТ, которая фокусировалась на 5 базовых компонентах: развитие информационной и коммуникационной инфраструктуры и повышение ее доступности, формирование человеческих ресурсов, развитие национальной отрасли разработки программного обеспечения, создание собственного контента на арабском языке и обеспечение информацией о Земле. Значительный акцент был сделан на формировании системы среднего образования, обеспечивающего необходимыми цифровыми навыками. Для реализации стратегии были созданы департаменты в профильных ведомствах и различные комитеты.

Национальная стратегия кибербезопасности отсутствует, система органов государственного управления в этой сфере не сформирована.

1 https://publicadministration.un.org/egovkb/Portals/egovkb/Documents/un/2020-Survey/2020%20UN%20E-Government%20Survey%20-%20Russian.pdf

3. Законодательство в сфере информационной безопасности

3.1. Закон о киберпреступности (2007)

Закон о противодействии киберпреступности[2] ратифицирован Президентом Республики в 2007 году. В соответствии с ним созданы специализированная прокуратура и подразделения полиции. Закон содержит 30 статей, 19 из которых предусматривают наказание за совершенные преступления и подстрекательство к указанным действиям.

Разделение глав закона происходит по субъекту преступления. Наказания за технологические преступления содержатся во второй главе, а за традиционные преступления в главах 3-6. В закон включаются:

а) преступления, которые совершаются в Интернете или информационной системе, где компьютер или система являются его средой, например, нарушение неприкосновенности частной жизни, угрозы, шантаж, нанесение ущерба репутации и т.д.;

б) преступления, в которых компьютер является инструментом, например, ограбление и отмывание денег;

в) преступления, целью которых является компьютер или система, например, уничтожение данных, нарушение работы операционных систем, распространение вредоносного программного обеспечения.

Также закон предусматривает уголовную ответственность до пяти лет лишения свободы и/или штраф за создание веб-сайтов, критикующих правительство или публикующих клеветнические материалы и контент, нарушающий общественную мораль или общественный порядок.

3.2. Закон о борьбе с киберспреступлениями (2018)

Нормативный акт разработан Министерством связи Судана с опорой на редакцию аналогичного закона от 2007 года и направлен на ужесточение контроля в сети Интернет. Полный текст закона не был опубликован на официальных ресурсах, но некоторые положения упоминались в прессе.[3]

Согласно отчету Комитета по законодательству, правосудию и правам человека закон включает дополнительные статьи, касающиеся разжигания ненависти в отношении иностранцев, и предусматривает наказание в виде двухлетнего тюремного заключения и/или штрафа для любого, кто использует информационно-коммуникационную сеть или любое средство информации для указанных выше действий, вызывая дискриминацию и враждебность.

2 https://ictpolicyafrica.org/en/document/oi11tiq4rq?page=1

3 https://sudanview.com/2018/06/11/المجلس-الوطني-يجيز-مشروع-قانون-جرائم-ا/

Закон включил в статью 23 наказания, связанные с распространением ложных новостей, так как было указано, что любой, кто использует информационную или коммуникационную сеть или любое из средств информации, связи или приложений для публикации любых новостей, слухов или сообщений, зная, что они не соответствуют действительности, с намерением вызвать страх или панику среди населения, угрожая общественной безопасности и подрывая престиж государства, наказывается тюремным заключением на срок не более одного года, телесным наказанием или штрафом.

В седьмой главе закона разделены статьи за преступления против детей и за преступления на почве дискриминации, похищение, заманивание и продажу детей и предусмотрено наказание до шести лет или штраф для любого, кто использует информационную сеть для угроз, запугивания, продажи и эксплуатации детей.

Статья 37 закона предусматривает наказание вплоть до пожизненного лишения свободы и штраф для любого, кто использует информационную сеть для заманивания ребенка, передачи его органов и использования его в сексуальной деятельности, оплачиваемой и неоплачиваемой, или на принудительных работах, или для подстрекательства к самоубийству. В своем отчете комитет указал, что закон состоит из 8 глав и 48 статей, по сравнению с 30-ю статьями в законе 2007 года.

Глава 2 закона включила положения, предусматривающие преступления в отношении сайтов, систем и сетей связи и коммуникационных услуг, проникновение на сайты и информационные системы третьих лиц, проникновение на сайты и информационные системы со стороны должностного лица, остановка, перехват, препятствование, нарушение, срыв и прослушивание доступа к услугам.

В 2020 году в закон внесены поправки, увеличившие тюремные сроки более чем в полтора раза.[4]

3.3. Закон об электронных транзакциях (2007)

Закон создал основы электронного документооборота в Судане. Он позволил всем финансовым учреждениям в стране предоставлять свои услуги через электронную систему, разрешил полное или частичное волеизъявление с помощью электронных средств.

Статья 8.1 Закона гласит: «Юридическая сила электронной подписи не может быть опровергнута с точки зрения ее действительности и возможности работать под ней только из-за ее полного или частичного воспроизведения в электронном формате». Статья 8.2 устанавливает: «Если закон требует подписания документа или обеспечивает юридическую силу в случае отсутствия подписи,

4 https://redress.org/wp-content/uploads/2020/07/2-Sudan-Amendments-July-2020-English-REDRESS-translation.pdf

если при этом используется электронная подпись, то электронная подпись удовлетворяет требованиям, предусмотренным настоящим законом».

Этим законом предусмотрено, что информация может быть доступна и извлечена в дальнейшем путем передачи, печати или иным способом, а также закон содержит статьи, регулирующие электронные инструменты и электронное исполнение, его подлинность и средства.

На основании положений закона создан Национальный комитет по электронной аутентификации, Министром юстиции сформирована Арбитражная комиссия для осуществления процесса обжалования решений органа в суде Национальной высшей инстанции.

4. Общие подходы к противодействию угрозам информационной безопасности, в том числе основные направления обеспечения информационной безопасности, включая используемые ключевые институты и инструменты защиты

В контексте борьбы с распространенными во всем мире угрозами информационной безопасности Судан использует следующие институты.

4.1. Национальный информационный центр

Национальный информационный центр (National Information Center, NIC[5]) является государственным органом, которым руководит Министерство связи и информационных технологий. Официально отвечает за кибербезопасность в Судане. Центр выступает и дает рекомендации государственным органам в области информационных технологий и формулирования государственной политики по развитию и продвижению информационных технологий в качестве международного инструмента для расширения доступа к информации. Он работает в нескольких секторах, таких как киберинфраструктура, программное обеспечение, стандарты и продвижение индустрии управления информацией. Одним из основных направлений деятельности NIC является проведение региональных мероприятий по распространению культуры кибербезопасности.

Центр также является координатором электронного правительства Судана. Национальный центр информационной безопасности работает в сотрудничестве с партнерами в различных государственных учреждениях для повышения доверия граждан Судана к услугам электронного правительства и обеспечения конфиденциальности и безопасности государственных данных на различных этапах обработки.

5 https://nic.gov.sd/

В структуре NIC существует Национальный центр программного обеспечения (National Software Center), который работает над организацией, локализацией и модернизацией индустрии программного обеспечения и его использования в Судане путем спонсирования и принятия новых инициатив и творческих идей, разработки и внедрения стандартов и стандартных систем, а также достижения лидерства в этой сфере.

4.2. Нильский центр технологических исследований

Нильский центр технологических исследований (Nile Center for Technology Research, NCTR[6]) был основан в 2007 году как первый научно-исследовательский центр в Судане, специализирующийся на ИКТ. В задачи центра входила разработка технологических решений для государственных учреждений с целью устранения пробелов, возникших в результате санкций против Судана. В 2012 году NCTR был зарегистрирован как частная компания и начал больше ориентироваться на бизнес. С момента своего создания NCTR предоставляет целый спектр ИКТ-решений в области кибербезопасности, сетей, коммуникаций, электроники и корпоративного программного обеспечения.

4.3. Национальная группа реагирования Sudan-CERT

Суданский центр информационной безопасности (Sudan CERT) был создан в январе 2010 г. по инициативе Управления по регулированию почтовых телекоммуникаций. Он представляет собой национальный центр, на который возложена задача повышения эффективности защиты в области информационной безопасности для всех национальных объектов, использующих ИКТ, и играет роль службы быстрого реагирования на инциденты информационной безопасности. Он представляет собой консультативный орган для граждан и компаний в области информационной безопасности.

В состав центра входят государственные органы и заинтересованные организации, например, Национальный информационный центр, телекоммуникационные компании, Нильский центр исследований.

Задачи центра:

а) работать в качестве механизма раннего предупреждения;

б) служить в качестве доверенного координационного центра;

в) осуществлять сбор статистической информации о сетевых инцидентах;

г) предоставлять периодические отчеты об угрозах;

д) оказывать помощь в проведении тренингов по гражданскому образованию для повышения осведомленности суданских граждан в вопросах ИТ-безопасности;

6 www.nctr.sd

е) отслеживать, тестировать и анализировать отчеты об угрозах;
ж)предоставлять судебно-экспертные услуги правоохранительным органам.

5. Участие в международном сотрудничестве в области формирования системы обеспечения международной информационной безопасности в рамках ООН и позиция при голосовании по наиболее важным резолюциям ГА ООН

Республика Судан поддержала российский проект резолюции Генеральной Ассамблеи ООН от 5 декабря 2018 г. A/RES/73/27 о переформатировании дискуссии по международной информационной безопасности в прозрачный, инклюзивный диалог и созыве РГОС.

Резолюция Генеральной Ассамблеи ООН A/RES/73/187 «Противодействие использованию информационно-коммуникационных технологий в преступных целях» от 17 декабря 2018 г. страной была поддержана.

Судан одобрил американский проект резолюции Генеральной Ассамблеи ООН «Поощрение ответственного поведения государств в киберпространстве в контексте международной безопасности» (A/RES/73/266 от 22 декабря 2018 г.).

6. Участие в международном сотрудничестве с другими международными организациями в области формирования системы обеспечения информационной безопасности на региональном уровне

Судан редко использует международное сотрудничество в сфере информационной безопасности. По сообщению органов власти,[7] в ноябре 2020 г. проведение семинаров по реформированию закона о борьбе с киберпреступностью было завершено. Семинар организовывался Министерством юстиции в координации и сотрудничестве с Европейским советом с участием руководителей министерства и соответствующих органов власти.

Нильский центр технологических исследований в ноябре 2020 г. принимал делегацию из посольства США, в ходе которой обсуждались пути возможного сотрудничества с американскими компаниями, что поддержит стратегическое развитие Центра и предоставит широкие возможности для ИКТ-сектора в Судане на следующем этапе.[8]

Суданский центр информационной безопасности (Sudan-CERT) является членом FIRST.[9]

7 https://moj.gov.sd/posts/post/600
8 https://www.nctr.sd/blog/visit-of-a-delegation-from-the-us-embassy/
9 https://www.first.org/members/teams/

7. Содержание и оценка предложений и инициатив в области формирования системы обеспечения международной информационной безопасности

В марте 2021 г., после исключения Судана из списка государств-спонсоров терроризма, был проведен Саммит SUDAN FUSION 2021. Саммит по цифровой трансформации Судана направлен на достижение интеграции государственного и частного секторов, а также на объединение правительства и бизнеса. В рамках мероприятия эксперты отрасли, бизнес-лидеры и поставщики решений собрались для изучения современных технологий, применения передового опыта, предоставления услуг и решений для граждан и национального бизнеса, которые поддерживают реформу национальной экономики. На саммите также обсуждались пути развития электронного правительства путем внедрения новейших технологий и возможности улучшения взаимодействия между правительством и гражданами.

Несмотря на возможное цифровое развитие государства, Закон о киберпреступности оказывает сдерживающее воздействие на свободу слова и свободу СМИ в Судане, в то время как доступ к информации является актуальной необходимостью. В связи с ограничениями, которые накладываются на журналистов и СМИ, Интернет является одной из платформ для обмена информацией и для доступа к ней. Для защиты свободы слова правительству Судана необходимо внести поправки в Закон о киберпреступности и привести его в соответствие с международными стандартами свободы выражения мнений.

22. ТУНИС

Официальное название: Тунисская Республика

Столица: Тунис

Официальные языки: арабский и французский

Территория: 163 610 км² (91-я в мире). По площади это самая маленькая страна Магриба. Площадь: общая — 163 610 км². Протяженность границ с Алжиром — 965 км, Ливией — 459 км. Береговая линия составляет 1148 км. Территориальные воды — 12 морских миль, исключительная экономическая зона — 200 морских миль (101 857 км²), континентальный шельф — 67 126 км².

Население: 11 658 341 чел. (по оценкам на 2019 год), что является 77-м показателем в мире.

Государственное устройство: В 2014 году в Тунисской Республике завершился переход к новой конституционной и политической системе, которая начала складываться после свержения авторитарного режима президента Зин аль-Абидина Бен Али в январе 2011 г. В январе 2014 г. Национальное учредительное собрание, сформированное в октябре 2011 г. по итогам первых свободных выборов, утвердило новую конституцию страны. Основной закон гарантирует соблюдение гражданских прав, свободу вероисповедания и устанавливает равенство мужчин и женщин перед законом. Новую конституцию Туниса называли одной из самых прогрессивных в арабском мире.

Экономика: Показатели ВВП (Паритет покупательной способности) за 2019 год:

- Итого: $131,087 млрд (82-й показатель в мире)
- На душу населения: $11 125 (109-й показатель в мире)

Показатели ВВП (Номинал) за 2019 год:

- Итого: $38,797 млрд (92-й показатель в мире)
- На душу населения: $3293 (125-й показатель в мире)

Дипломатические отношения с Россией (СССР): установлены 11 июля 1956 г.

1. Уровень развития системы обеспечения информационной безопасности и информационно-коммуникационной инфраструктуры (включая индекс развития ИКТ по оценкам МСЭ и ООН)

Исходя из статистических данных, уровень развития системы информационной безопасности Туниса может быть оценен как средний:

МСЭ 2021, индекс кибербезопасности: 86,2 (из 100)

МСЭ 2021, позиция в рейтинге среди государств-членов ЛАГ: 6

МСЭ 2021, позиция в глобальном рейтинге: 45

МСЭ, уровень проникновения Интернет: 68,44%

NCSI, уровень цифрового развития: 46,26

NCSI, индекс готовности предотвращать киберугрозы и реагировать: 46,75

2. Основные документы стратегического планирования в области обеспечения информационной безопасности

Национальная Стратегия кибербезопасности Туниса на 2020–2025 годы.[1]

Принята в 2018 году, направлена на защиту и развитие национального киберпространства посредством наращивания киберпотенциала. Согласно Стратегии национальное и цифровое доверие должно обеспечиваться во взаимодействии с набором отраслевых и частных стратегий, параллельно с реализацией планов на местах и при координации со всеми участвующими сторонами.

Цели Стратегии:

- продвижение совместной работы между всеми, кто участвует в ИКТ-отрасли, и поддержка координации между ними;
- предотвращение киберугроз и обеспечение устойчивости путем укрепления национального киберпотенциала, повышения осведомленности и защиты жизненно важных информационных инфраструктур;
- поддержка цифрового доверия путем внедрения необходимых механизмов и процедур для этой цели;
- достижение лидерства в цифровой сфере путем создания безопасной цифровой среды и получение приоритета на региональном и международном уровнях;
- международное сотрудничество, достижение баланса между международным сотрудничеством и обеспечением высших интересов государства.

Закон № 5-2004 от 3 февраля 2004 г.[2] о компьютерной безопасности и организации сферы компьютерной безопасности.

1 https://ncss.ansi.tn/

2 https://www.ansi.tn/sites/default/files/loi%205-2004%20FR.pdf

- устанавливает общие правила защиты компьютерных систем и сетей. Закон № 63-2004 от 27 июля 2004 г. о защите персональных данных[3].

Уголовный кодекс, 1999 год.[4]

Статья 199-бис: определяет мошеннический доступ к автоматизированной системе обработки данных; модификацию или уничтожение функционирования системы или существующих данных; умышленное изменение или нарушение функционирования автоматизированной системы обработки данных; мошенническое внесение данных в автоматизированную систему обработки данных.

Статья 199-тер: определяет модификацию содержания электронного документа, причиняющую вред.

Постановление № 1250-2004 от 25 мая 2004 г.[5] Определяет компьютерные системы и сети организаций, подлежащих периодическому обязательному аудиту компьютерной безопасности, а также критерии, касающиеся характера аудита и его периодичности, процедуры его проведения, контроль за применением рекомендаций, содержащихся в аудиторском заключении.

В Тунисе действует ряд отраслевых Циркуляров по информационной безопасности:

- Циркуляр № 24[6](2020 год) — касается улучшения и оптимизации мер ИТ-безопасности на уровне публичных компаний.
- Циркуляр № 23[7](2020 год) — касается управления официальными аккаунтами публичных компаний в социальных сетях.
- Циркуляр № 19[8](2007 год) — об усилении мер компьютерной безопасности в общественных учреждениях (создание отдела технической безопасности, назначение начальника по безопасности информационных систем и создание руководящего комитета).

Проект Цифрового кодекса[9] (август 2018 г.)

В сентябре 2018 г. начались обсуждения нового «Цифрового кодекса» с целью исправления, улучшения или дополнения элементов законопроекта по электронным сообщениям.

Третья книга — «Защита национального цифрового пространства» была разделена на четыре раздела:

1) «Национальная стратегия цифровой безопасности».

2) «Национальное агентство информационной безопасности».

3 https://www.ansi.tn/sites/default/files/loi%20organique%202004-63.pdf
4 https://www.ansi.tn/sites/default/files/loi%2099-89.pdf
5 https://www.ansi.tn/sites/default/files/d%c3%a9cret%202004-1250%20fr.pdf
6 https://www.ansi.tn/sites/default/files/Circulaire%2024%20nov%202020%20.pdf
7 https://www.ansi.tn/sites/default/files/Circulaire%2023%20nov%202020.pdf
8 https://www.ansi.tn/sites/default/files/circulaire%2007-19_2.pdf
9 https://www.ansi.tn/sites/default/files/Code_pour_une_Tunisie_Numerique.pdf

3) «Защита чувствительных и динамических цифровых инфраструктур».

4) «Защита системы и безопасность сети».

Национальная Стратегия Туниса по Искусственному интеллекту[10]. В основном направлена на определение оперативных целей, по сферам: исследования, экосистема, инфраструктура, управление, кадры, финансирование, большие данные.

Цели Стратегии:

- использовать ИИ в качестве базы формирования ценностей;
- сделать Тунис источником талантливых кадров в области ИИ;
- обеспечить благоприятные условия для создания процветающей экосистемы ИИ.

Стратегия предполагает развитие:

- ценностей, ориентированных на человека и справедливость;
- критериев прозрачности и объяснимости;
- инвестирования в ИИ.

Дорожная карта по Искусственному интеллекту[11] устанавливает цели и предлагает план действий по развитию ИИ в Тунисе:

- повысить осведомленность о реальных проблемах и возможностях ИИ;
- развивать культуру и демистифицировать ИИ, чтобы облегчить его освоение;
- повышать осведомленность о влиянии на трансформацию рабочих мест и необходимых навыках «завтрашнего дня»;
- понять существующие ловушки ИИ;
- укреплять экосистему для развития ИИ;
- развивать навыки ИИ;
- разработать инфраструктуру, в т.ч. облачные технологии;
- продвигать сетевую активность;
- реализовать пилотные проекты в области ИИ в государственном и частном секторах;
- развивать инициативы в области открытых инноваций;
- продвигать методы ИИ;
- сформулировать национальную стратегию в области ИИ;
- принять национальный план действий в области ИИ на 2021–2025 годы.

Политика в области IP-адресов для Искусственного Интеллекта[12] действует для защиты алгоритмов ИИ в качестве объектов интеллектуальной собственности.

10 https://oecd.ai/en/dashboards/policy-initiatives/http:%2F%2Faipo.oecd.org%2F2021-data-policyInitiatives-27128
11 https://oecd.ai/en/dashboards/policy-initiatives/http:%2F%2Faipo.oecd.org%2F2021-data-policyInitiatives-27126
12 https://oecd.ai/en/dashboards/policy-initiatives/http:%2F%2Faipo.oecd.org%2F2021-data-policyInitiatives-27133

Политика доступа к информации[13] (принята на базе Закона № 2011-41 от 26 мая 2011 г., касающегося доступа к административным документам государственных органов) действует в целях раскрытия правительственных данных в ключевых секторах для повышения качества услуг, а также с тем, чтобы улучшить процесс принятия решений на основе ИИ, снизить предвзятость принимаемых решений и стимулировать конкуренцию между поставщиками услуг.

3. Основные угрозы информационной безопасности и общие подходы к противодействию этим угрозам, в том числе основные направления обеспечения информационной безопасности, включая используемые ключевые институты и инструменты защиты

В качестве новых киберугроз в Тунисе отмечаются[14]:

- нарушения безопасности КИИ;
- DeepWeb — Интернет, не индексируемый традиционными поисковыми системами;
- Dark Net — частные нелегальные сети;
- Dark Web — адреса, размещенные в Dark Net;
- проблемы защиты больших данных;
- кибератаки с использованием передовых технологий, таких как распределенные системы обнаружения вторжений (D-IDS), сети-ловушки (Honeynet) и датчики вредоносного трафика (сенсоры).

В качестве ключевого института по обеспечению информационной безопасности в Тунисе действует Национальное агентство компьютерной безопасности[15] (ANSI), как национальный координатор, работает над созданием климата доверия к информационным технологиям, чтобы «успокоить» пользователей, государство и инвесторов и защитить граждан, государственную и частную собственность от любых киберугроз.

Стратегия ANSI основана на пяти стратегических направлениях:

- Укрепить безопасность национального киберпространства от киберрисков и угроз.
- Усилить защиту национальных информационных систем.
- Содействовать развитию адекватной нормативно-правовой базы.
- Создать культуру кибербезопасности высокого уровня.
- Установить партнерские отношения с академическими исследовательскими структурами и частным сектором.

13 https://oecd.ai/en/dashboards/policy-initiatives/http:%2F%2Faipo.oecd.org%2F2021-data-policyInitiatives-27131
14 https://www.itu.int/en/ITU-T/Workshops-and-Seminars/cybersecurity/Documents/PPT/S7P2_Nadhir_L.pdf
15 https://www.ansi.tn/ar

ANSI осуществляет общий контроль над компьютерными системами и сетями, принадлежащими различным государственным и частным организациям, а также отвечает за следующие задачи:

- Обеспечить выполнение национальных целей и общей стратегии в системах безопасности компьютерных систем и сетей.
- Контролировать выполнение планов и программ, связанных с компьютерной безопасностью в государственном секторе, за исключением приложений, специфичных для обороны и национальной безопасности, и обеспечивать координацию между заинтересованными сторонами в этой области.
- Обеспечить технологическую охрану в области компьютерной безопасности.
- Установить конкретные стандарты ИТ-безопасности и разработать технические руководства в этой сфере.
- Работать над поощрением национальных решений в области компьютерной безопасности и их продвижением в соответствии с приоритетами и программами, которые будут установлены агентством.
- Участвовать в обучении и переподготовке в области компьютерной безопасности.
- Обеспечить выполнение правил, касающихся обязательности периодической проверки безопасности компьютерных систем и сетей.

Группа реагирования на компьютерные чрезвычайные ситуации[16] (TunCERT). Действует под эгидой Национального агентства компьютерной безопасности, представляет собой Центр помощи и поддержки в области компьютерной безопасности (через горячую линию, доступную 24 часа в сутки, для сбора заявлений об инцидентах безопасности и / или кибератаках, а также для любого вида технической помощи пользователям и администраторам).

Безвозмездно оказывает необходимую помощь как гражданам, так и специалистам по всем вопросам, связанным с безопасностью информационных систем, и обеспечивает наличие соответствующих средств, способных обеспечить защиту национального киберпространства Туниса.

Ставит одной из целей информирование об инцидентах и привлечение внимания национального и регионального сообщества к угрозам информационной безопасности к руководству в отношении средств защиты от них.

Стремится помочь Интернет-сообществу правильно использовать ИТ-технологии и системы, продвигать обучение высокого уровня в различных областях безопасности информационных систем и облегчать общение между профессионалами и экспертами, работающими в области информационной безопасности.

16 https://www.ansi.tn/fr/tuncert/presentation

Стремится организовывать мероприятия и дискуссионные форумы, способствовать возникновению ассоциаций, специализирующихся в области компьютерной безопасности.

Центр обмена и анализа информации SAHER[17] создан в результате многолетнего мониторинга защиты КИИ Национальным агентством по компьютерной безопасности (ANSI) и группой TunCERT.

Основными функциями Центра являются сбор, анализ и обмен событиями, связанными с кибербезопасностью.

Среди задач Центра:

- Измерение уровня защиты национального киберпространства путем извлечения глобальных индикаторов, информирующих о потенциальных угрозах.
- Предоставление платформы для мониторинга кибератак и предложить поддержку в расследовании инцидентов, связанных с компьютерной безопасностью.
- Внедрение и разрабатывать решения для обнаружения и отслеживания кибератак с использованием передовых технологий, таких как распределенные системы обнаружения вторжений (D-IDS), сети-ловушки (Honeynet) и датчики вредоносного трафика (сенсоры).
- Мониторинг критически важных узлов, таких как серверы Интернет-провайдеров (DNS, Mail) и интернет-маршрутизаторы, для обнаружения аномалий и вторжений, которые могут возникнуть в результате кибератак.
- Обнаружение атак, нацеленных на веб-сайты, размещенные в национальном киберпространстве. Действительно, веб-приложения являются первыми объектами атак, особенно сайты электронной коммерции, представляющие экономические интересы.
- Разработка системы обнаружения распространения вирусов (вирусы, ботнеты) в национальном масштабе для выявления источников заражения, типов вредоносных программ и контроллеров ботов, а также внедрить механизмы очистки путем обмена источниками данных с Интернет-провайдерами.
- Создание базы знаний (типы атак, эксплойты, источники атак, черные списки, целевые порты, эксплуатируемые уязвимости), которые составляют общие ресурсы.
- Улучшеине возможности наблюдения и обнаружения, чтобы обеспечить лучшую видимость в киберпространстве.

17 https://www.ansi.tn/fr/ANSI/SAHER

4. Участие в международном сотрудничестве в области формирования системы обеспечения международной информационной безопасности в рамках ООН и позиция при голосовании по наиболее важным резолюциям ГА ООН

Тунис в целом поддерживает российские инициативы в области международной информационной безопасности.

В 2018–2020 годах проголосовал за принятие российских проектов резолюций Генеральной Ассамблеи ООН:

A/RES/73/27 от 5 декабря 2018 г. (принятие правил, норм и принципов ответственного поведения, а также создание Рабочей группы ООН открытого состава);

A/RES/75/240 от 31 декабря 2020 г. (создание новой Рабочей группы ООН открытого состава по вопросам безопасности в сфере использования ИКТ и самих ИКТ 2021–2025).

Вместе с тем Тунис воздержался при голосовании по российскому проекту резолюции Генеральной Ассамблеи ООН:

A/RES/74/247 от 27 декабря 2019 г. (создание специального межправительственного комитета экспертов открытого состава для разработки всеобъемлющей международной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях). Также не голосовал по российскому проекту резолюции Генеральной Ассамблеи ООН:

- A/RES/73/187 от 17 декабря 2018 г. (включение в повестку дня ООН обсуждения вопроса о противодействии использованию ИКТ в преступных целях).
- Тунис проголосовал за принятие американского проекта резолюции Генеральной Ассамблеи ООН A/RES/73/266 от 22 декабря 2018 г. (о создании Группы правительственных экспертов ООН на 2019–2021 годы).

5. Участие в международном сотрудничестве с другими международными организациями в области формирования системы обеспечения информационной безопасности на региональном уровне

Тунис взаимодействует на глобальном и региональном уровнях по вопросам обеспечения кибербезопасности в рамках следующих международных организаций, членом которых он является:

ООН;

ITU (МСЭ);

Движение неприсоединения;

Африканский союз;

ЛАГ;

Интерпол;

ISO (Международная организация по стандартизации).

В ноябре 2017 г. подписано Соглашение о сотрудничестве в области безопасности информационных систем между Тунисом и Францией.[18]

В 2015 году была подписана Декларация о намерениях между Тунисом и Испанией[19], которая включает в себя совместную работу в международных и региональных организациях, а также с общими партнерами и союзниками.

Тунис участвует в проекте CyberSouth[20]– Сотрудничество в борьбе с киберпреступностью в регионе южного соседства, проект ЕС по предотвращению и борьбе с киберпреступлениями и другими правонарушениями, связанными с электронными доказательствами, в соответствии с международными стандартами и передовой практикой в области прав человека и верховенства права.

Тунис зарегистрирован в качестве члена Глобального форума по киберэкспертизе[21]- глобальная платформа для стран, международных организаций и частных компаний для обмена опытом и знаниями по наращиванию киберпотенциала.

В декабре 2020 г. Национальное агентство по ИТ-безопасности приняло участие в семинарах, организованных Министерством коммуникационных технологий в сотрудничестве с Немецким агентством международного сотрудничества[22]. Это участие является частью реализации плана действий национальной стратегии кибербезопасности.

Группа чрезвычайного реагирования TunCERT является членом FIRST[23] с 15 мая 2007 г., а также членом UNCTAD[24], OIC-CERT[25] и HONEYNET[26].

18 https://www.ssi.gouv.fr/actualite/la-france-et-la-tunisie-signent-un-accord-de-cooperation-dans-le-domaine-de-la-cybersecurite/

19 https://thediplomatinspain.com/en/2017/05/spain-will-sign-with-india-its-seventh-agreement-on-cybersecurity-since-2015/

20 https://www.euneighbours.eu/en/south/stay-informed/projects/project-cybersouth-cooperation-cybercrime-southern-neighbourhood

21 https://thegfce.org/member/tunisia/

22 https://www.ansi.tn/fr/formation/manifestations-realisees/workshops-dans-le-cadre-de-la-mise-en-place-du-plan-daction-de-la

23 https://www.first.org/

24 https://unctad.org/

25 https://www.oic-cert.org/en/

26 https://www.honeynet.org/

6. Содержание и оценка предложений и инициатив в области формирования системы обеспечения международной информационной безопасности

Тунис:

присоединился к инициативе Франции — Парижский призыв к доверию и безопасности в киберпространстве (2018 год);

не стал соавтором инициативы Франции и Египта — Программа действий ООН по продвижению ответственного поведения государств в киберпространстве (2020 год).

Список основных используемых сокращений

АС – Африканский союз

ВВП – Валовой внутренний продукт

ГА ООН – Генеральная Ассамблея Организации Объединенных Наций

ГПЭ ООН –

в 2004–2017 годах: Группа правительственных экспертов ООН по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности

в 2019–2021 годах: Группа правительственных экспертов ООН по поощрению ответственного поведения государств в киберпространстве в контексте международной безопасности

ЕС – Европейский союз

ИИ – Искусственный интеллект

ИКТ – Информационно-коммуникационные технологии

КИИ – Критическая информационная инфраструктура

ЛАГ – Лига арабских государств

МИБ – Международная информационная безопасность

МСЭ (ITU) – Международный союз электросвязи

НАТО – Организация Североатлантического договора

ОБСЕ – Организация по безопасности и сотрудничеству в Европе

ООН – Организация Объединенных Наций

РГОС ООН –

в 2019–2021 годах: Рабочая группа ООН открытого состава по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности

в 2021–2025 годах: Рабочая группа ООН открытого состава по вопросам безопасности в сфере использования информационно-коммуникационных технологий и самих информационно-коммуникационных технологий 2021–2025

ССАГПЗ – Совет сотрудничества арабских государств Персидского залива

ЮНИДИР – Институт Организации Объединенных Наций по исследованию проблем разоружения

CERT – Группа реагирования на компьютерные чрезвычайные ситуации

CSIRT – Группа реагирования на инциденты компьютерной безопасности

(в докладе Группа правительственных экспертов по поощрению ответственного поведения государств в киберпространстве в контексте международной безопасности 2021 года):

CERT – Группа реагирования на компьютерные инциденты

CSIRT – Группа реагирования на инциденты информационной безопасности

(в Резюме Председателя к докладу Рабочей группы открытого состава по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности 2021 года):

CERTs – Группы реагирования на компьютерные инциденты

CSIRTs – Группы реагирования на инциденты в сфере компьютерной безопасности

СБОРНИК МАТЕРИАЛОВ ПО ПРОБЛЕМАТИКЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ГОСУДАРСТВ-ЧЛЕНОВ ЛИГИ АРАБСКИХ ГОСУДАРСТВ

Подписано в печать 06.03.2023. Гарнитура Times.
Формат 60x84/8. Объем 28,37 усл. печ. л.
Тираж 100 экз.