ВЕСТНИК
Кемеровского государственного университета
полититические, социологические и экономические науки

оригинальная статья

Система национальной кибербезопасности Саудовской Аравии: специфика и риски развития

Леонид Вячеславович Цуканов
Уральский федеральный университет имени Первого Президента России Б. Н. Ельцина, Россия, г. Екатеринбург; https://orcid.org/0000-0001-6882-9841; leon.tsukanov@mail.ru

Поступила в редакцию 31.08.2021. Принята после рецензирования 27.09.21. Принята в печать 15.11.2021.

Аннотация: В статье рассматриваются особенности системы обеспечения национальной кибербезопасности Королевства Саудовская Аравия. Опираясь на стандарты кибербезопасности, разработанные Международным союзом электросвязи при ООН, раскрыты институционально-правовые основы саудовской системы, определена степень вовлеченности страны в международное сотрудничество по вопросам защиты глобального и национального киберпространства, выявлены ключевые риски развития архитектуры саудовской кибербезопасности. Автор приходит к выводу, что в вопросах цифровой защиты Саудовская Аравия придерживается догоняющей модели развития и, несмотря на положительную оценку ее деятельности со стороны Международного союза электросвязи, по-прежнему испытывает некоторые проблемы с защитой национального киберпространства как общемирового характера (например, пробелы в законодательстве), так и обусловленного спецификой национальной модели управления государством. В числе наиболее явных рисков развития цифровой защиты страны выделены дисбаланс между ее гражданским и военным секторами, наличие определенных разногласий между ее различными субъектами, слабая интегрированность местного хакерского сообщества в общую структуру национальной кибербезопасности. По мнению автора, Эр-Рияд нацелен на устранение указанных дисбалансов и в среднесрочной перспективе намерен выстроить комплексную систему кибербезопасности с опорой на расширение международного сотрудничества в области развития национальной и региональной цифровой среды и методов ее эффективной защиты.
Ключевые слова: информационная безопасность, цифровая защита, киберпреступность, стратегии цифрового развития, Видение 2030, государственно-частное партнерство, международное сотрудничество

Цитирование: Цуканов Л. В. Система национальной кибербезопасности Саудовской Аравии: специфика и риски развития // Вестник Кемеровского государственного университета. Серия: Политические, социологические и экономические науки. 2021. Т. 6. № 4. С. 435–443. https://doi.org/10.21603/2500-3372-2021-6-4-435-443

Введение

Одним из ключевых трендов развития современных государств в последние годы стало значительное повышение роли киберфактора в обеспечении национальной и международной безопасности. Особую актуальность проблема противостояния киберугрозам приобретает для стран Ближнего Востока, где стремительная цифровизация всех сфер жизни общества усиливает и без того высокий конфликтный потенциал региона. Научное осмысление опыта строительства системы национальной кибербезопасности Королевства Саудовская Аравия позволяет выявить специфику и риски развития цифровой защиты не только указанной страны, претендующей на региональное лидерство, но и целого ряда ближневосточных государств, в первую очередь аравийских монархий, сталкивающихся со схожим комплексом угроз и вызовов, исходящих из киберпространства.

О значимости саудовского опыта свидетельствуют показатели Глобального индекса кибербезопасности (GCI), разработанные исследовательским мегапроектом Международного союза электросвязи (МСЭ) при ООН. Так, если в 2014 г. Саудовская Аравия занимала по степени цифровой защищенности 19 место в мировом рейтинге и 6 место среди государств Персидского залива[1], то уже в 2018 г. – 13 и 2 места соответственно[2], а по итогам 2020 г. вышла на вторую строку глобального рейтинга, уступая лишь США и став абсолютным лидером не только ближневосточного региона, но также арабских стран и исламского мира[3]. Подробный расклад актуализирует ряд вопросов: какова специфика развития системы цифровой защиты Королевства? Какие факторы обусловили успех саудовского подхода к обеспечению национальной кибербезопасности? С какими рисками развития система сталкивается в настоящем?

[1] Global Cybersecurity Index. Oyster Bay: ABI Research; ITU, 2014. 15 p.

[2] Global Cybersecurity Index (GCI) 2018. Geneva: ITU, 2019. 92 p.

[3] Global Cybersecurity Index 2020. Geneva: ITU, 2021. 172 p.

ВЕСТНИК
Кемеровского государственного университета
полититические, социологические и экономические науки
https://doi.org/10.21603/2500-3372-2021-6-4-435-443

Проблематика национальной и международной кибербезопасности представлена в современном научном поле внушительным количеством исследований и характеризуется высокой степенью дискуссионности ввиду разнообразия методологических подходов. Однако российские и зарубежные эксперты сходятся во мнении, что каждое государство нарабатывает собственные практики цифровой защиты, обусловленные спецификой национального развития [1, с. 22–27]. Ведущие российские востоковеды-арабисты, как правило, обращаются к проблемам цифрового развития Королевства в рамках фундаментальных исследований особенностей социально-политического развития [2, с. 128–130] и реализации стратегической программы модернизации страны «Видение 2030» [3, с. 61–62; 4, с. 39–41]. Саудовский опыт формирования эффективной системы кибербезопасности пока не стал предметом отдельного исследования, хотя определенные наработки представлены в трудах израильских [5, p. 32–34] и американских [6, p. 108–109] политологов. Данная статья в определенной степени позволяет восполнить указанный пробел.

Источниковой базой статьи стали документы профильных министерств и ведомств Саудовской Аравии, отражающие концептуальные подходы страны к обеспечению национальной цифровой защиты; отчеты международных организаций, ведущих экспертных центров и IT-компаний, специализирующихся на вопросах кибербезопасности; интервью саудовских политиков; материалы информационно-новостных ресурсов арабских стран.

В основу анализа специфики и рисков развития саудовской системы кибербезопасности положены критерии, разработанные МСЭ для определения степени цифровой защищенности государств: нормативно-правовая база и институты реализации киберполитики; технические возможности; государственно-частное партнерство, международное сотрудничество, кадровый потенциал[4].

Институционально-правовые основы саудовской системы национальной кибербезопасности

Подключение Саудовской Аравии к Интернету в 1997 г. поставило в национальную повестку вопрос о внесении корректив в нормативно-правовую базу страны с учетом новых цифровых реалий. В течение следующего десятилетия был принят целый ряд законов и постановлений, регламентирующих поведение пользователей в киберпространстве. К наиболее значимым документам относятся Закон о порядке деятельности интернет-провайдеров 1999 г., Постановление о телекоммуникациях и Акт о порядке использования Интернета и спутниковой связи 2002 г., Закон об отмене дуополии на предоставление услуг сотовой связи и упрощенном использовании протоколов GPRS и GMPCS 2006 г., Закон о борьбе с преступлениями в киберпространстве 2007 г.[5] и др. [7, p. 278].

Одновременно начинается процесс формирования институтов, призванных осуществлять на практике имплементацию профильных законов. В 2001 г. создается Комиссия по коммуникациям и информационным технологиям (Комиссия), которая стала регулировать данную сферу, а также инициировала в 2005 г. несколько значимых проектов (электронное правительство [8, p. 305–309], развитие инфраструктуры открытых ключей[6], инициатива «Домашний компьютер»[7] и др.), повлекших за собой расширение полномочий и функционала целого ряда органов государственной власти [9, p. 345]. Наряду с Комиссией были сформированы такие важные специализированные институты цифровой безопасности, как Национальный центр цифровой сертификации, Киберполиция и др.

Следует признать, что до 2011 г. строительство национальной системы кибербезопасности имело импульсивный характер, шло скачкообразно, без следования какому-либо долгосрочному плану. Ведомства (в первую очередь министерства обороны, внутренних дел, иностранных дел, связи, экономики) по мере появления новых цифровых угроз и вызовов расширяли свой функционал, инициируя разработку и введение новых нормативных документов. Однако взаимодействие между институтами практически сводилось к минимуму. Отсутствие целостного подхода к обеспечению цифровой безопасности можно объяснить тем, что до событий Арабской весны, продемонстрировавших значимость новейших технологий для мобилизации протестного ресурса и политической борьбы в целом, саудовские власти не относили угрозы из киберпространства к угрозам высшего уровня.

Уже в 2012 г. Эр-Рияд представил проект Стратегии национальной информационной безопасности (Стратегии), подготовленный при участии Министерства связи и информационных технологий (Минсвязи) и Комиссии [10, p. 49]. В документе суммировались все законодательные наработки 1999–2007 гг., а также впервые подчеркивалась важность стабильности цифровой сферы для экономического процветания страны. Мощным импульсом к разработке комплексного подхода к обеспечению национальной кибербезопасности стало принятие в 2016 г.

[4] Global Cybersecurity Index…

[5] Service Regulations // Communications and Information Technology Commission. Режим доступа: https://www.citc.gov.sa/en/RulesandSystems/RegulatoryDocuments/Licenses/CITCLicensingGeneralSpecialConditions/Pages/default.aspx (дата обращения: 13.08.2021).

[6] Ba-Isa M. Y. Saudi PKI project making progress // Arab News. 14.04.2009. Режим доступа: https://www.arabnews.com/node/323231 (дата обращения: 17.08.2021).

[7] Hassan J. CITC to promote computer literacy among Saudi families // Arab News. 09.07.2005. Режим доступа: https://www.arabnews.com/node/269741 (дата обращения: 15.08.2021).

долгосрочной стратегии модернизации Саудовской Аравии «Видение 2030», где цифровым технологиям отводилась роль одного из ключевых драйверов прорывного развития Королевства.

В 2017 г. было создано Национальное управление кибербезопасности (Управление) – главный институт, регулирующий обеспечение безопасности цифровой инфраструктуры Королевства в гражданском секторе[8]. В октябре 2018 г. Управление опубликовало первый регламент, содержащий список базовых требований к госучреждениям в области обеспечения цифровой защиты [11]. Особое внимание было уделено защите критической инфраструктуры страны, в первую очередь – ее нефтегазовых комплексов [12, p. 30]. В этой связи Управление начинает закупки зарубежного ПО, которые к 2020 г. приобрели централизованный и постоянный характер [13, p. 49].

Также в 2017 г. при участии Управления были обновлены положения Стратегии [10, p. 51–52]. В соответствии с новой трактовкой первоочередными целями стали институционализация системы национальной кибербезопасности и выработка новых подходов к цифровизации, ориентированных на развитие национальной smart-экономики. Примечательно, что Стратегия по сей день существует в формате проекта: ее окончательному принятию препятствуют разногласия между военными и гражданскими ведомствами относительно разграничения сфер ответственности. Тем не менее эксперты рассматривают этот документ как главный ориентир для Эр-Рияда при выстраивании политики в цифровом пространстве [14, p. 9].

Развитие системы профильных институтов, ускоренное в связи с реализацией «Видения 2030», позволило перераспределить и конкретизировать функционал различных министерств, а также укрепить межведомственное взаимодействие. Так, например, Минсвязи связи передало Управлению часть своих надзорных функций, что позволило первому сосредоточиться на доработке запущенных ранее нацпроектов в области цифровой безопасности, прежде всего проекта электронного правительства, дополненного многоцелевой инициативой «Yesser»[9]. Создание Национального департамента оцифровки, специализирующегося на разработке и внедрении инструментов цифровой экономики, способствовало внушительному укреплению технического потенциала национальной кибербезопасности [15, p. 165–166]. Даже с учетом того, что Эр-Рияд продолжает делать ставку на зарубежное ПО, данный процесс свидетельствует о непрекращающемся укреплении структур, контролирующих технические аспекты цифровой отрасли Королевства.

Международное сотрудничество

Международное сотрудничество является одним из ключевых элементов саудовской системы кибербезопасности, поскольку позволяет стране не только интегрироваться в качестве полноправного субъекта в глобальные и региональные процессы, связанные с созданием безопасной цифровой среды, но и аккумулировать ресурсы для развития государственно-частного партнерства и собственного кадрового и технического потенциала.

МСЭ стал первой международной площадкой, в рамках которой началась интеграция Саудовской Аравии в глобальное цифровое сообщество, в том числе путем адаптации национальной стратегии и политики цифрового развития к мировым стандартам [16]. Кроме того, Королевство представлено на других площадках, осуществляющих цифровое взаимодействие между государствами, – в специализированных рабочих группах ООН, Организации Исламского Сотрудничества, Лиге Арабских Государств (ЛАГ). Саудовские специалисты также регулярно принимают участие в цифровых учениях, проводимых на региональном (Cyber Polygon, OIC-CERT Cybersecurity Drill) и глобальном (ITU Global Cyber Drills) уровнях [17, с. 454]. Важным шагом к укреплению технического потенциала Саудовской Аравии стало присоединение к международной Компьютерной группе реагирования на чрезвычайные ситуации (CERT), которое позволило Эр-Рияду оперативно принять стандарты, разработанные МСЭ [18, с. 6–7].

Арабский региональный центр кибербезопасности, открытый в 2012 г. под эгидой МСЭ, на сегодняшний день является для Саудовской Аравии главной платформой для развития международного партнерства, поскольку позволяет сконцентрироваться на выстраивании коллективной кибербезопасности в рамках Совета сотрудничества арабских государств Персидского залива (ССАГПЗ).

Тенденция к постепенному обособлению региона в вопросах цифровой защиты является общей для всех стран ССАГПЗ и частично обусловлена разногласиями со странами ЛАГ по части толкования терминов *информационная безопасность* и *кибербезопасность*. Саудовская Аравия, как и большинство государств ССАГПЗ, придерживается западного подхода к определению вышеупомянутых понятий: *информационная безопасность* сводится преимущественно к техническим проблемам контроля и соблюдения законности и правопорядка в телекоммуникационной сфере (защита от несанкционированного доступа и хакерских взломов компьютерных сетей и сайтов, компьютерных вирусов и вредоносных программ и т. п.) [18, с. 8]. Социально-политические аспекты цифровой защиты (например,

[8] Rasooldeen M. Saudi Arabia sets up new commission to boost cybersecurity // Arab News. 02.11.2017. Режим доступа: https://www.arabnews.com/node/1186926/saudi-arabia (дата обращения: 17.08.2021).

[9] Digital Government Authority // GOV.SA. Режим доступа: https://www.my.gov.sa/wps/portal/snp/main (дата обращения: 10.08.2021); Yesser // E-Government Program. Режим доступа: https://www.yesser.gov.sa/en (дата обращения: 10.08.2021).

ВЕСТНИК
Кемеровского государственного университета
полититические, социологические и экономические науки
https://doi.org/10.21603/2500-3372-2021-6-4-435-443

противодействие использованию информационно-коммуникационных технологий в качестве инструмента дестабилизации общества), как правило, находятся вне рамок саудовского паттерна.

Международное партнерство дает Саудовской Аравии импульс к развитию собственного кадрового потенциала, являющегося одним из главных критериев эффективности национальных систем кибербезопасности. В 2020 г. цифровая отрасль Королевства испытывает дефицит кадров на уровне 20–25 %, который планируется преодолеть к 2030 г. [19, с. 45]. С 2017 г. растет число образовательных учреждений, осуществляющих подготовку специалистов в области информационной безопасности. Подобные программы открыты в ведущих вузах страны (Университет Дар Аль-Хекма, Саудовский электронный университет и т. д.) и реализуются в партнерстве с зарубежными университетами и аналитическими центрами [20]. Университет науки и технологий имени короля Абдаллы разрабатывает программы профессиональной переподготовки госслужащих, чья деятельность связана с кибербезопасностью [21].

Международное сотрудничество создает благоприятные условия и для развития государственно-частного партнерства. В 2020 г. в Королевстве зарегистрировано около десятка IT-компаний, работающих в сфере кибербезопасности и оказывающих государству консультационные и технические услуги (AlJammaz Technologies, Innovative Solutions, Taqnia Cyber и др.)[10]. Эксперты ожидают, что сотрудничество государства с деловыми кругами будет расширяться и дальше, в том числе посредством разработки и продвижения таких национальных цифровых брендов в рамках проектов «Видения 2030», как, например, знаменитый проект города будущего Неом [22, p. 429–431].

Эр-Рияд уверенно берет курс на превращение страны в мировой центр кибербезопасности. В 2020 г. Королевство стало принимающей стороной первого Глобального форума по кибербезопасности, миссия которого – консолидировать усилия мирового сообщества в вопросах выработки новых решений в области кибербезопасности[11]. Проведение Форума позволило укрепитьцифровой имидж страны, а также наметить новые направления международного сотрудничества в цифровой сфере [23, p. 1021].

Риски развития национальной кибербезопасности

Развитие системы национальной кибербезопасности Саудовской Аравии сталкивается с комплексом угроз и рисков, часть которых характерна для всех государств мира, а часть исходит из специфики внутреннего развития Королевства. В первую очередь многие страны сталкиваются с инертностью законодательной сферы, что в условиях стремительного развития цифровой инфраструктуры объективно ведет к образованию лакун в нормативно-правовом поле.

Весьма показателен Закон о борьбе с киберпреступлениями (2007 г.)[12]. С одной стороны, он по-прежнему является основным регулятором в вопросах пресечения данного вида правонарушений и позволяет закрывать некоторые лакуны, а, с другой стороны, не предусматривает механизма противодействия новым видам преступлений, которые постоянно появляются (кибербуллинг, цифровой шантаж и др.) [24, p. 100–102]. В свою очередь законопроекты, направленные на купирование отдельных аспектов проблемы (например, Инициатива Минсвязи по повышению осведомленности о кибербуллинге и борьбе с ним 2020 г.[13]), обеспечивают лишь временный эффект и не способствуют борьбе с киберпреступлениями в целом. Более того, бюрократизация и создание большого количества актов-приложений вместо обновления базовых законов усложняют противодействие угрозам и ведут к формированию незащищенных сегментов в архитектуре национальной кибербезопасности.

В случае с Эр-Риядом ситуация также усугубляется необходимостью согласования законодательных инициатив с ортодоксальным духовенством. С момента появления в стране Интернета саудовскими богословами было выпущено 42 фетвы: 16 из них оценивали развитие цифровой инфраструктуры как свойственную времени тенденцию, 19 – как негативное явление, в 7 фетвах не было сформулировано однозначной оценки [25, p. 200–205]. Даже Совет высших улемов за этот период выпустил несколько предписаний, содержащих противоположные оценки ускоряющейся цифровизации саудовского общества. Как итог, однозначная позиция ортодоксального духовенства (пусть и в гибких формулировках) не обозначена (что довольно нетипично для данного государства) [26, p. 35]: это ведет к формированию дуализма восприятий стратегий и проектов «Видения 2030» и усугубляет разногласия между сторонниками и противниками цифровизации страны.

[10] Saudi Arabia // Cyber Security Intelligence. Режим доступа: https://www.cybersecurityintelligence.com/location/saudi-arabia/ (дата обращения: 17.08.2021).

[11] Saudi Arabia to Host Global Cybersecurity Forum in February // Asharq Al-Awsat. 21.10.2019. Режим доступа: https://english.aawsat.com//home/article/1955151/saudi-arabia-host-global-cybersecurity-forum-february (дата обращения: 17.08.2021).

[12] Anti-Cyber Crime Law, tr. Saudi Laws. Promulgated by Royal Decree 8 Mar 1428 No. M/17, as amended 26 Mar 2007 // WIPO Lex. Режим доступа: https://wipolex.wipo.int/en/text/328209 (дата обращения: 10.08.2021).

[13] MCIT launches initiative to raise awareness on cyberbullying // Saudi Gazette. 11.11.2020. Режим доступа: http://www.mcit.gov.sa/en/campaigns/cyberbulling (дата обращения: 13.08.2021).

Отсутствие координации между отдельными субъектами кибербезопасности (прежде всего между гражданскими и военными) является еще одним риском на пути выстраивания комплексной системы национальной цифровой защиты. На сегодняшний день Саудовская Аравия демонстрирует высокий уровень милитаризации, что в значительной степени обусловлено стремлением Эр-Рияда к региональному лидерству. В Глобальном индексе военной мощи страна занимает 17 место в мире (4 – в регионе), а по объемам военных расходов – 7 место в мире (1 – в регионе)[14].

При этом, как известно, военный потенциал современного государства все больше определяется наличием высокоточных вооружений и использованием цифровых технологий в военной сфере. Соответственно, национальный киберпотенциал складывается из показателей гражданского и военного секторов. Однако в Королевстве военные аспекты кибербезопасности развиваются без участия гражданских специалистов, что ведет к отсутствию единой стратегии цифровой защиты страны.

Кроме того, Саудовская Аравия вовлечена в гибридный конфликт с Ираном, который ведется в том числе с использованием цифровых инструментов воздействия, например, в форме хакерских атак на объекты критической инфраструктуры противника. При этом, по мнению зарубежных исследователей, Эр-Рияд практически не уделяет внимания развитию наступательного аспекта кибероборонны: по сути, саудовские силовые ведомства реагируют на цифровые угрозы постфактум [5, p. 35–37]. В целом дисбаланс в развитии военной и гражданской кибербезопасности является фактором, значительно ослабляющим цифровую защиту государства в целом.

Значимым субъектом кибербезопасности являются хакерские сообщества, деятельность которых, в отличие от ряда других стран Ближнего Востока, не регулируется госструктурами Королевства. Патриотично настроенные саудовские хакерские группировки, объединенные под общим названием «Кибермухи» (Cyber-Flies), хотя и действуют в интересах Эр-Рияда, руководствуются собственным пониманием политических приоритетов страны. Нередко это приводит к казусам: так, в январе – феврале 2021 г. группа хакеров, причисляющих себя к «Кибермухам», осуществила серию кибератак на аккаунты иранских официальных лиц[15], а в июле 2021 г. нанесла удар по цифровой инфраструктуре Министерства дорог и транспорта Ирана[16]. Оба инцидента были восприняты Тегераном как грубое нарушение достигнутых ранее с Эр-Риядом договоренностей, что негативно повлияло на процесс двусторонних консультаций по вопросам региональной безопасности [27, p. 789–790].

Отдельную группу рисков сформировала пандемия COVID-19. С переходом большинства служащих на удаленный режим работы нагрузка на национальные сети выросла в десятки раз, что увеличило их уязвимость к хакерским атакам. Согласно отчетам Лаборатории Касперского, в 2020 г. цифровая инфраструктура Саудовской Аравии подверглась 22,5 млн кибератак (30 % – успешные), а в первой половине 2021 г. – 7 млн атак (37 % – успешные)[17]. Как отмечают эксперты, наиболее распространенный вид кибернападений – DDoS-атака, которая относится к категории средств грубой силы и не требует от исполнителя выдающихся навыков. Примечательно, что по сравнению с предыдущим годом число таких атак выросло на 104 %[18], что свидетельствует о наличие значительных недостатков в системе обеспечения кибербезопасности.

Заключение

Успех Саудовской Аравии, которой удалось в относительно короткие сроки выстроить эффективную систему защиты национального киберпространства, обусловлен комплексом фактором. В их числе следует отметить стабильность режима и наличие политической воли у правящей элиты, ориентированной на интеграцию Королевства в глобальные экономические и политические процессы в качестве одного из передовых государств мира. По сути, курс на формирование национальной системы кибербезопасности стал составной частью саудовской стратегии модернизации страны «Видение 2030», что обеспечило всей цифровой сфере Королевства поступательное развитие под контролем властей. Также необходимо подчеркнуть значительную роль международного сотрудничества, благодаря которому саудовские власти смогли довольно быстро нарастить технический и кадровый потенциал страны, запустить высокотехнологичные проекты в рамках государственно-частного партнерства в области национальной цифровой безопасности.

Вместе с тем в вопросах цифровой защиты Саудовская Аравия продолжает придерживаться догоняющей модели, в рамках которой предпочитает закупать за рубежом уже готовые решения, нежели разрабатывать

[14] 2021 Military Strength Ranking // GFP. Режим доступа: https://www.globalfirepower.com/countries-listing.php (дата обращения: 17.08.2021).

[15] Farmanfarmaian R., Mens J. In the Middle East, war is going digital // Foreign Policy. 22.02.2021. Режим доступа: https://foreignpolicy.com/2021/02/22/in-the-middle-east-war-is-going-digital/ (дата обращения: 15.08.2021).

[16] Holmes D. Iran transport ministry hit by second apparent cyberattack in days // Reuters. 10.07.2021. Режим доступа: https://www.reuters.com/world/middle-east/iran-transport-ministry-hit-by-second-apparent-cyberattack-days-2021-07-10/ (дата обращения: 17.08.2021).

[17] Emm D. What does 2021 have in store for cybersecurity? // Kaspersky. 22.12.2020. Режим доступа: https://www.kaspersky.com/blog/secure-futures-magazine/cybersecurity-predictions-2021/38136/ (дата обращения: 17.08.2021).

[18] Там же.

ВЕСТНИК
Кемеровского государственного университета
полититические, социологические и экономические науки
https://doi.org/10.21603/2500-3372-2021-6-4-435-443

собственные цифровые продукты. Устойчивость саудовской системы кибербезопасности, кроме того, подвергается рискам в связи с относительно низким уровнем взаимодействия между различными субъектами национальной кибербезопасности, представляющими интересы гражданского и военного секторов, правительственных ведомств, негосударственных акторов и т. д.

Можно ожидать, что в силу стратегической значимости «Видения 2030» и растущих региональных амбиций Саудовское королевство сделает выбор в пользу комплексного подхода к развитию национальной кибербезопасности, продолжив поддержку ее гражданского сегмента с одновременным укреплением военного аспекта цифровой защиты страны. Не исключено, что для гармонизации собственной киберсистемы Саудовская Аравия воспользуется передовым опытом США, своего традиционного геополитического союзника, а также Израиля, отношения с которым вышли недавно на качественно новый уровень. В целом траектории и динамика дальнейшего развития системы цифровой защиты Королевства, как и ранее, в значительной степени будут определяться комплексом внутриполитических, региональных и глобальных факторов.

Конфликт интересов: Автор заявил об отсутствии потенциальных конфликтов интересов в отношении исследования, авторства и / или публикации данной статьи.

Литература

1. Лебедева М. М., Харкевич М. В., Зиновьева Е. С., Копосова Е. Н. Архаизация государства: роль современных информационных технологий // Полис. Политические исследования. 2016. № 6. С. 22–36. https://doi.org/10.17976/jpps/2016.06.03
2. Сапронова М. А. Арабский восток на современном этапе: эволюция институтов власти и модернизация традиционного общества // Вестник Томского государственного университета. 2009. № 318. С. 125–132.
3. Косач Г. Г. Саудовская Аравия: трансформация власти и политики // Мировая экономика и международные отношения. 2019. Т. 63. № 4. С. 59–67. https://doi.org/10.20542/0131-2227-2019-63-4-59-67
4. Мелкумян Е. С. Развитие арабских монархий залива: прорыв в будущее // Азия и Африка сегодня. 2020. № 2. С. 37–42. https://doi.org/10.31857/S032150750008471-0
5. Easttom C., Butler W. The Iran-Saudi cyber conflict // International Journal of Cyber Warfare and Terrorism. 2021. Vol. 11. № 2. P. 29–42. https://doi.org/10.4018/IJCWT.2021040103
6. Nodelend B., Morris R. The impact of low self-control on past and future cyber offending // International Journal of Cyber Criminology. 2020. Vol. 14. № 1. P. 106–120. https://doi.org/10.5281/zenodo.3742075
7. Polat A. Effects of GDPR on the financial services sector in the Kingdom of Saudi Arabia //Journal of Data Protection & Privacy. 2021. Vol. 4. № 3. P. 273–282.
8. Alrubaiq A., Alharbi T. Developing a cybersecurity framework for e-government project in the Kingdom of Saudi Arabia // Journal of Cybersecurity and Privacy. 2021. Vol. 1. № 2. P. 302–318. https://doi.org/10.3390/jcp1020017
9. Albogami O., Alruqi M., Almalki K., Aljahdali A. Public key infrastructure traditional and modern implementation // International Journal of Network Security. 2021. Vol. 23. № 2. P. 343–350. https://doi.org/10.6633/IJNS.202103_23(2).18
10. Abu-Taieh E., Alfaries A. A., Al-Otaibi S., Aldehim G. Cyber security crime and punishment: comparative study of the laws of Jordan, Kuwait, Qatar, Oman, and Saudi Arabia // International Journal of Cyber Warfare and Terrorism. 2018. Vol. 8. № 3. P. 46–59. https://doi.org/10.4018/IJCWT.2018070104
11. NSCA strength and conditioning professional standards and guidelines // Strength and Conditioning Journal. 2017. Vol. 39. № 6. P. 1–24. https://doi.org/10.1519/SSC.0000000000000348
12. Al-Mulhim R. A., Al-Zamil L. A., Al-Dossary F. M. Cyber-attacks on Saudi Arabia environment // International Journal of Computer Networks and Communications Security. 2020. Vol. 8. № 3. P. 26–31. https://doi.org/10.47277/IJCNCS/8(3)1
13. Ali A. M., Shamsuddin S. M., Eassa F. E., Saeed F., Alassafi M. O., Al-Hadhrami T., Elmisery A. M. Towards an intelligent framework for cloud service discovery // International Journal of Cloud Applications and Computing. 2021. Vol. 11. № 3. P. 33–57. https://doi.org/10.4018/IJCAC.2021070103
14. Alzubaidi A. Measuring the level of cyber-security awareness for cybercrime in Saudi Arabia // Heliyon. 2021. Vol. 7. № 1. https://doi.org/10.1016/j.heliyon.2021.e06016
15. Mahmood H. The security challenges in cloud IoT – a review // Saudi Journal of Engineering and Technology. 2021. Vol. 6. № 7. P. 162–168. https://doi.org/10.36348/sjet.2021.v06i07.003
16. Arab States call for heightened cybersecurity // ITU News. 2008. № 3. P. 32. Режим доступа: https://historicjournals.itu.int/viewer/516/?return=1&css-name=include#page=34&viewer=picture&o=&n=0&q= (дата обращения: 14.08.2021).
17. Шкваря Л. В. Интеграционные процессы в ССАГПЗ в условиях цифровизации // Экономика и предпринимательство. 2020. № 11. С. 453–455. https://doi.org/10.34925/EIP.2020.124.11.082

18. Валиахметова Г. Н. Ближний Восток в цифровую эпоху: глобализация угроз региональной безопасности // Восток (Oriens). 2017. № 3. С. 6–15.
19. Леонова О. Г. Кибервойна и противоборство в цифровом информационном пространстве // Информационное общество. 2018. № 2. С. 43–46.
20. Almomani I., Ahmed M., Maglaras L. Cybersecurity maturity assessment framework for higher education institutions in Saudi Arabia // PeerJ Computer Science. 2021. Vol. 7. https://doi.org/10.7717/peerj-cs.703
21. Alammary A., Alshaikh M., Alhogail A. The impact of the COVID-19 pandemic on the adoption of e-learning among academics in Saudi Arabia // Behaviour & Information Technology. 2021. https://doi.org/10.1080/0144929x.2021.1973106
22. Ouassini A., Boynton K. W. The «Silicon Valley of the Middle East»: cybersecurity, Saudi Arabia, and the path to Vision 2030 // Routledge Companion to Global Cyber-Security Strategy / eds. S. N. Romaniuk, M. Manjikian. 1st ed. London: Routledge, 2021. P. 427–434. https://doi.org/10.4324/9780429399718-36
23. Aleidan M. Commercial diplomacy as a part of national transformation and its impact on the internationalization of SMEs: evidence from Saudi Arabia // Asian Economic and Financial Review. 2019. Vol. 9. № 9. P. 1019–1031. 10.18488/journal.aefr.2019.99.1019.1031
24. Albantan M. A. R. Social skills and cyberbullying behavior among students in Hail from the perspective of social work // Cypriot Journal of Educational Sciences. 2021. Vol. 16. № 1. P. 96–113. https://doi.org/10.18844/cjes.v16i1.5512
25. Soliman N. S. The direct fatwa in the media, the pros and cons // Islamic Sciences Journal. 2020. Vol. 11. № 10. P. 192–221. http://dx.doi.org/10.25130/islam.v11i10.379
26. Mowatt-Larssen R. Zawahiri's WMD fatwa. Symmetry between 2003 WMD fatwa and 2008 «Exoneration» // Islam and the Bomb: Religious Justification For and Against Nuclear Weapons. Cambridge: Belfer Center for Science and International Affairs, 2011. P. 35–37.
27. Ahmadian H., Mohseni P. From detente to containment: the emergence of Iran's new Saudi strategy // International Affairs. 2021. Vol. 97. № 3. P. 779–799. https://doi.org/10.1093/ia/iiab014

original article

Saudi Arabia National Cyber Security System: Specificity and Development Risks

Leonid V. Tsukanov

B. N. Yeltsin Ural Federal University, Russia, Yekaterinburg; https://orcid.org/0000-0001-6882-9841; leon.tsukanov@mail.ru

Received 31 Aug 2021. Accepted after peer review 27 Sep 2021. Accepted for publication 15 Nov 2021.

Abstract: The research featured the national cybersecurity system of the Kingdom of Saudi Arabia. The cybersecurity standards developed by the International Telecommunication Union of the United Nations made it possible to reveal the institutional and legal foundations of the digital security system, as well as the degree of involvement in international cybersecurity cooperation. The analysis demonstrated the key risks of the development of the Saudi cyber model. The assessment by the International Telecommunication Union standards gave quite positive results. However, Saudi Arabia proved to adhere to a catching-up development model and still experiences some problems with national cyberspace security. Some are of global nature, e.g. legislation gaps, while others result from the specifics of the national model of state governance. The most obvious risks include the imbalance between the civil and military sectors, the disagreements between various regions, and the poor integration of the local hacker community into the overall structure of national cybersecurity. Saudi Arabia plans to eliminate these imbalances in the medium term in order to build an integrated cybersecurity system by expanding its international cooperation.

Keywords: information security, digital protection, cybercrime, digital development strategies, Vision 2030, public-private partnerships, international cooperation

Citation: Tsukanov L. V. Saudi Arabia National Cyber Security System: Specificity and Development Risks. *Vestnik Kemerovskogo gosudarstvennogo universiteta. Seriia: Politicheskie, sotsiologicheskie i ekonomicheskie nauki*, 2021, 6(4): 435–433. (In Russ.) https://doi.org/10.21603/2500-3372-2021-6-4-435-443

Conflict of interests: The author declared no potential conflict of interests regarding the research, authorship, and / or publication of this article.

References

1. Lebedeva M. M., Kharkevich M. V., Zinovieva E. S., Koposova E. N. State archaization: the role of information technologies. *Polis. Political Studies*, 2016, (6): 22–36. (In Russ.) https://doi.org/10.17976/jpps/2016.06.03
2. Sapronova M. A. The Arab East on the modern stage: evolution of institutions of power and modernization of traditional society. *Vestnik Tomskogo gosudarstvennogo universiteta*, 2009, (318): 125–132. (In Russ.)
3. Kosach G. G. Saudi Arabia: transformation of power and policy. *Mirovaya ekonomika i mezhdunarodnye otnosheniya,* 2019, 63(4): 59–67. (In Russ.) https://doi.org/10.20542/0131-2227-2019-63-4-59-67
4. Melkumyan E. S. Development of Arab gulf monarchies: breakout to future. *Aziya i Afrika segodnya*, 2020, (2): 37–42. (In Russ.) https://doi.org/10.31857/S032150750008471-0
5. Easttom C., Butler W. The Iran-Saudi cyber conflict. *International Journal of Cyber Warfare and Terrorism*, 2021, 11(2): 29–42. https://doi.org/10.4018/IJCWT.2021040103
6. Nodelend B., Morris R. The impact of low self-control on past and future cyber offending. *International Journal of Cyber Criminology*, 2020, 14(1): 106–120. https://doi.org/10.5281/zenodo.3742075
7. Polat A. Effects of GDPR on the financial services sector in the Kingdom of Saudi Arabia. *Journal of Data Protection & Privacy*, 2021, 4(3): 273–282.
8. Alrubaiq A., Alharbi T. Developing a cybersecurity framework for e-government project in the Kingdom of Saudi Arabia. *Journal of Cybersecurity and Privacy,* 2021, 1(2): 302–318. https://doi.org/10.3390/jcp1020017
9. Albogami O., Alruqi M., Almalki K., Aljahdali A. Public key infrastructure traditional and modern implementation. *International Journal of Network Security*, 2021, 23(2): 343–350. https://doi.org/10.6633/IJNS.202103_23(2).18
10. Abu-Taieh E., Alfaries A. A., Al-Otaibi S., Aldehim G. Cyber security crime and punishment: comparative study of the laws of Jordan, Kuwait, Qatar, Oman, and Saudi Arabia. *International Journal of Cyber Warfare and Terrorism,* 2018, 8(3): 46–59. https://doi.org/10.4018/IJCWT.2018070104
11. NSCA strength and conditioning professional standards and guidelines. *Strength and Conditioning Journal,* 2017, 39(6): 1–24. https://doi.org/10.1519/SSC.0000000000000348
12. Al-Mulhim R. A., Al-Zamil L. A., Al-Dossary F. M. Cyber-attacks on Saudi Arabia environment. *International Journal of Computer Networks and Communications Security,* 2020, 8(3): 26–31. https://doi.org/10.47277/IJCNCS/8(3)1
13. Ali A. M., Shamsuddin S. M., Eassa F. E., Saeed F., Alassafi M. O., Al-Hadhrami T., Elmisery A. M. Towards an intelligent framework for cloud service discovery. *International Journal of Cloud Applications and Computing*, 2021, 11(3): 33–57. https://doi.org/10.4018/IJCAC.2021070103
14. Alzubaidi A. Measuring the level of cyber-security awareness for cybercrime in Saudi Arabia. *Heliyon*, 2021, 7(1). https://doi.org/10.1016/j.heliyon.2021.e06016
15. Mahmood H. The security challenges in cloud IoT – a review. *Saudi Journal of Engineering and Technology*, 2021, 6(7): 162–168. https://doi.org/10.36348/sjet.2021.v06i07.003
16. Arab States call for heightened cybersecurity. *ITU News*, 2008, (3): 32. Available at: https://historicjournals.itu.int/viewer/516/?return=1&css-name=include#page=34&viewer=picture&o=&n=0&q= (accessed 14 Aug 2021).
17. Shkvarya L. V. Integration processes in the GCC in the context of digitalization. *Ekonomika i predprinimatelstvo,* 2020, (11): 453–455. (In Russ.) https://doi.org/10.34925/EIP.2020.124.11.082
18. Valiakhmetova G. N. The Middle East in digital age: globalization of threats to regional security. *Vostok (Oriens)*, 2017, (3): 6–15. (In Russ.)
19. Leonova O. G. Cyber war and confrontation in the digital information space. *Informatsionnoye obshchestvo,* 2018, (2): 43–46. (In Russ.)
20. Almomani I., Ahmed M., Maglaras L. Cybersecurity maturity assessment framework for higher education institutions in Saudi Arabia. *PeerJ Computer Science,* 2021, 7. https://doi.org/10.7717/peerj-cs.703
21. Alammary A., Alshaikh M., Alhogail A. The impact of the COVID-19 pandemic on the adoption of e-learning among academics in Saudi Arabia. *Behaviour & Information Technology*, 2021. https://doi.org/10.1080/0144929x.2021.1973106
22. Ouassini A., Boynton K. W. The "Silicon Valley of the Middle East": cybersecurity, Saudi Arabia, and the path to Vision 2030. *Routledge Companion to Global Cyber-Security Strategy*, eds. Romaniuk S. N., Manjikian M., 1st ed. London: Routledge, 2021, 427–434. https://doi.org/10.4324/9780429399718-36
23. Aleidan M. Commercial diplomacy as a part of national transformation and its impact on the internationalization of SMEs: evidence from Saudi Arabia. *Asian Economic and Financial Review*, 2019, 9(9): 1019–1031. 10.18488/journal.aefr.2019.99.1019.1031

24. Albantan M. A. R. Social skills and cyberbullying behavior among students in Hail from the perspective of social work. *Cypriot Journal of Educational Sciences*, 2021, 16(1): 96–113. https://doi.org/10.18844/cjes.v16i1.5512
25. Soliman N. S. The direct fatwa in the media, the pros and cons. *Islamic Sciences Journal*, 2020, 11(10): 192–221. http://dx.doi.org/10.25130/islam.v11i10.379
26. Mowatt-Larssen R. Zawahiri's WMD fatwa. Symmetry between 2003 WMD fatwa and 2008 "Exoneration". *Islam and the Bomb: Religious Justification For and Against Nuclear Weapons*. Cambridge: Belfer Center for Science and International Affairs, 2011, 35–37.
27. Ahmadian H., Mohseni P. From detente to containment: the emergence of Iran's new Saudi strategy. *International Affairs*, 2021, 97(3): 779–799. https://doi.org/10.1093/ia/iiab014