Доверие и безопасность в информационном обществе

ОСНОВНЫЕ ПРОБЛЕМЫ КИБЕРБЕЗОПАСНОСТИ НА БЛИЖНЕМ ВОСТОКЕ

Статья рекомендована к публикации членом редакционного совета А. А. Стрельцовым 15.02.2024.

Емелин Данил Романович

Московский государственный университет имени М. В. Ломоносова, факультет глобальных процессов, аспирант
Москва, Российская Федерация
danil.emelin@mail.ru

Аннотация

С развитием информационных технологий кибербезопасность приобрела первостепенную значимость для поддержания стабильности политических процессов, происходящих на международной арене. Конфликты между государствами переместились в совершенно новое измерение – информационное. При этом обеспечение безопасности информационного пространства, развитие соответствующих институциональных структур разнится от региона к региону. В этой связи Ближний Восток, будучи одним из самых нестабильных регионов мира, сталкивается с уникальными вызовами в сфере кибербезопасности, которые проявляются как в экономической, так и геополитической сущности международных процессов. Автор рассматривает основные проблемы, а также подходы к реализации политики в сфере кибербезопасности стран ближневосточного региона.

Ключевые слова

Ближний Восток, кибербезопасность, информационное общество, глобализация, региональная безопасность, кибертерроризм

Введение

Современная мировая политика характеризуется тесным уровнем взаимосвязи и взаимозависимости акторов международных отношений, которого без развития единого информационного пространства в глобальном понимании достичь невозможно. С появлением в 1990-х годах сети Интернет трансформация политических процессов и экономических потоков достигла небывалых масштабов, что, в свою очередь, поставило перед всеми государствами проблему поддержания международной информационной безопасности. При этом, если обратить внимание на структуру глобального информационного пространства, то можно заметить его схожесть с обычной политической картой ввиду повсеместного возникновения информационных войн между различными державами, а также целенаправленной политики, ограничивающей доступ к информации.

В этой связи кибербезопасность представляет собой один из важнейших факторов для поддержания стабильности всей системы международных отношений. Тем не менее, до сих пор существует некоторая неопределенность в том, что подразумевается под самим термином «кибербезопасность». Причина подобного заключается в недостаточно изученной природе самого феномена. Если ранее «кибербезопасность» означала защиту отдельных компьютерных систем, то на сегодняшний день это стратегическое направление в обеспечении национальной безопасности.

В частности, в Доктрине информационной безопасности Российской Федерации «кибербезопасность» понимается как «состояние защищенности её национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства» [16]. Также в отечественной литературе подчеркивается, что

Производство и хостинг журнала «Информационное общество» осуществляется Институтом развития информационного общества.

https://doi.org/10.52605/16059921_2024_05_123

существующие запросы и противоречия в обществе активно проходят этап трансформации ввиду широкого доступа к информационным технологиям. В свою очередь, эти запросы порождают необходимость создавать соответствующие системы, которые позволяют вести информационные войны. По этой причине за последнее время значительно выросло количество стран, которые замечены в создании специализированных средств оказания влияния в этой области [8].

В зарубежной литературе под понятием «кибербезопасности» понимается «деятельность, необходимая для защиты сетей и информации, пользователей информационных сетей и иных сторон, которые могут быть затронуты киберугрозами».

Подобные структуры, в частности американские и британские, уже активно действуют в глобальных масштабах. Тем не менее, подавляющая часть подобных групп не подчиняется какому-либо правительству, что представляет собой нарастающую опасность для глобальной безопасности. С другой стороны, тема развития информационных средств оказания воздействия государствами зачастую становится неким манипулятивным приёмом для оказания давления. К такому приёму неоднократно прибегали страны Запада, говоря о так называемой российской «угрозе». Кроме того, террористические группировки также активно проявляют интерес к подобным системам.

Всё это подчеркивает значимость развития средств по противоборству информационным системам воздействия на критическую инфраструктуру, от которой зависит выживаемость государства в современном мире. Тем не менее, степень вовлеченности в развитие этого направления разнится от региона к региону.

1 Цифровизация Ближнего Востока

Ближний Восток занимает особое положение в системе международной безопасности ввиду того факта, что данному региону присуща высокая степень конфликтогенного потенциала. По сей день между множеством ближневосточных стран остаются нерешаемые проблемы на протяжении десятилетий, что несет прямую угрозу стабильности как для региональных держав, так и для всего международного сообщества из-за взаимосвязанности международных субъектов. К наиболее распространённым угрозам, исходящим из этого региона, относятся международный терроризм и связанная с ним проблема распространения различных видов вооружений, в том числе и массового поражения [6].

Также развитие Ближнего Востока и происходящие здесь процессы положили начало концепции «черного лебедя», разработанной Нассимом Николасом Талебом [9]. Под «черным лебедем» подразумевается, с одной стороны, некоторое событие, беспрецедентное по своему характеру, оказывающее влияние на все возможные сферы жизнедеятельности человека в том или ином регионе мира, но, с другой стороны, данное событие оказывается единственно возможным и закономерным по своей сущности. В данном контексте Ближний Восток является «лидером» по количеству таких событий: Арабская весна, ядерная программа Ирана, палестино-израильский конфликт в его текущем состоянии. Тем не менее, несмотря на существование предпосылок, свидетельствующих о таком «чёрном лебеде», предсказать его возникновение практически невозможно.

В данном контексте появление сети Интернет аналогичным образом сказалось и на Ближнем Востоке. Следствием данного события стало расширение процесса цифровизации на ближневосточный театр. Этот термин глубоко проник в нашу жизнь и внес ощутимые корректировки во всю структуру организации отношений внутри современного общества; тем не менее, ему всё ещё присуща множественность трактовок. Впервые понятие «цифровизация» было использовано Николасом Негропонте, который понимал его в связке с информатикой, а не с экономической сферой. По Негропонте цифровизация – социокультурный феномен, переход к которому чреват углублением проблем, связанных с обеспечением информационной безопасности [7].

Ряд отечественных авторов, в частности Герасимова Т.А. и Москвитина Н.В., рассматривают данный феномен с экономической точки зрения, где цифровизация представляет собой «процесс, включающий внедрение и использование инновационных технологий, а также принципы цифровой экономики в контексте социально-экономической жизни общества, сопровождающейся абсолютной автоматизацией, роботизацией и внедрением искусственного интеллекта», а также как «создание и применение современных систем, технологий и инструментов в целях повышения эффективности управленческих решений и предлагаемых услуг» [3].

В то же время цифровизация проявляется и в социальной плоскости, где Гайворонская Я. В. и Мирошниченко О. И. приписывают данному понятию несколько значений: «переход с аналоговой формы передачи информации на цифровую; оцифровывание информации», перевод информации в цифровой формат для последующего хранения, распространения и использования; широкий комплекс экономических, управленческих, социальных процессов, связанных с использованием и широким распространением собственно цифровых, компьютерных, информационных, электронных и сетевых (телекоммуникационных) технологий, а также систем искусственного интеллекта в современной жизни» [2].

В зарубежной литературе цифровизация трактуется как «процесс использования цифровых технологий и информации для трансформации экономических, социальных, политических и др. процессов» [18].

Что же касается данного процесса на Ближнем Востоке, то в последнее десятилетие регион подвергся колоссальным изменениям. Подавляющее число государств занимают лидирующие позиции по внедрению информационных технологий в социо-экономическую составляющую. С учетом развития инфраструктуры за последние несколько лет прослеживается существенный рост пользователей сети Интернет, что, в свою очередь, сказывается на увеличении арабоязычного контента по всему миру – за последнее десятилетие данный показатель вырос в 25 раз [14].

Первоначальные последствия цифровизации носили исключительно негативный характер. Именно ближневосточный регион стал той территорией, где впервые начались информационные войны. После восстания палестинских арабов против притеснений со стороны израильского правительства, так называемой «антифадой Аль-Акса», а также возложенной ответственностью на ряд государств Ближнего Востока за террористические акты 11 сентября 2001 года [1], ближневосточные государства испытали шквал информационного воздействия, который заключался в попытках манипулировать общественным сознанием, целенаправленном распространении ложных новостей и неоднократных попытках очернить правительства неугодных стран. Кроме того, в период Арабской весны ядерная программа Ирана подверглась беспрецедентной атаке со стороны Соединенных Штатов и Израиля при помощи разработанного вредоносного программного обеспечения, что подчеркнуло важность обеспечения информационной безопасности в глобальных масштабах. Исходя из всего вышесказанного, характерной чертой современного этапа цифровизации Ближнего Востока является наличие в этом процессе аналогичных проблем, как и для развития системы региональной безопасности, а именно: традиционные конфликты и противостояния «на земле» между региональными акторами перекочевали и в информационную сферу.

2 Основные проблемы кибербезопасности

На сегодняшний день формирование единого информационного пространства Ближнего Востока испытывает аналогичные проблемы, что и процесс становления системы региональной безопасности. Существенное влияние на динамику данного процесса оказывают как региональные, так и внерегиональные государства. Как и в случае с реализацией совместных подходов к развитию системы региональной безопасности, общей позиции по продвижению безопасности в киберпространстве в ближневосточном регионе добиться крайне затруднительно.

Причиной подобного является растущее количество кибератак на критическую инфраструктуру между региональными игроками, а также небывалый уровень кибершпионажа, что привело к росту количества средств информационного воздействия наступательного характера [15]. Однако уровень киберзащищенности стран Ближнего Востока тесно связан с уровнем экономического развития региональных акторов существенно отличаются между собой [17]. По этой причине единственными гарантами устойчивости системы цифровой безопасности Ближнего Востока являются ведущие государства региона, среди которых можно выделить Саудовская Аравия, Объединённые Арабские Эмираты и Иран. Баланс интересов между данными акторами призван открыть путь к дальнейшему становлению всей этой сложной системы.

В то же время данный процесс осложняется кардинально отличающимися подходами к определению структуры региональной системы информационной безопасности. В конечном счете это приводит к очередному блоковому режиму, препятствующим решению проблем в области кибербезопасности.

В частности, здесь прослеживается противостояние Ирана и Саудовской Аравии, которые развивают кардинально отличные друг от друга системы безопасности: Саудовская Аравия тесно взаимодействует в информационном пространстве с наиболее влиятельными игроками региона – с Объединенными Арабскими Эмиратами и Израилем (процесс нормализации взаимоотношений до очередной эскалации палестино-израильского конфликта), в то время как Иран делает ставку на неклассических акторов, среди которых можно выделить множество различных группировок.

Другим существенным препятствием на пути формирования эффективной системы кибербезопасности на ближневосточном пространстве является проблема кибератак на критическую инфраструктуру региональных акторов, задействованных в добыче экспортируемых полезных ископаемых – нефти и газа, а также тех государств, по территории которых проходят логические цепочки. В свою очередь любые потенциальные атаки на магистрали и нефтяные и газовые месторождения прямым образом угрожают и установленным ценам на углеводороды на международном рынке.

На фоне таких угроз вложения в кибербезопасность, согласно различным прогнозам аналитических центров, вырастит практически в 1,5 раза – до 22,4 млрд долларов США к 2028 году [16]. Этому способствует развивающаяся система стартапов, базирующейся на применении облачных технологий.

3 Подходы ближневосточных стран к обеспечению кибербезопасности в современных условиях

Иран

Движущей силой развития кибербезопасности в Иране стала кибератака на инфраструктуру его ядерной программы, организованная при взаимодействии США и Израиля. Помимо этого, данный региональный актор чаще других подвержен различным кибератакам – около 10% всех атак в мире приходится именно на Иран [4]. Учитывая агрессивную среду, Иран вынужден вкладываться в развитие систем информационного воздействия, что приносит свои результаты. Если ранее наступательные действия в информационной сфере носили больше показательный характер, в частности, хакерские атаки, то сегодня Иран проводит действительно масштабные операции. После эскалации конфликта между Палестиной и Израилем иранские организации, связанные с Корпусом стражей исламской революции, неоднократно взламывали систему противовоздушной обороны «Железный купол». Существенной проблемой на пути реализации своей политики в информационном пространстве является наличие сложной внутриполитической обстановки – постоянные протесты, а также последние события, связанные с гибелью президента Ибрахима Раиси. Тем не менее, Иран считается государством с высоким уровнем развития компетенций по обеспечению информационной безопасности наравне с Россией, Китаем и США.

Саудовская Аравия

Среди всех остальных государств ближневосточного региона Саудовская Аравия выступает в роли лидера не только в области экономики [8], но и в сфере обеспечения информационной безопасности. Если около 10 лет назад страна не входила даже в десятку по данному критерию, то сегодня она активно развивает институциональную базу для проведения соответствующей политики в сфере кибербезопасности на государственном уровне. Также именно Саудовская Аравия активно продвигает международное сотрудничество посредством специализированных организаций, к примеру органа ООН, специализирующегося на противодействии кибератакам и кибертерроризму, а также некоторых интеграционных объединений регионального уровня. Развитие взаимоотношений с развитыми странами по направлению информационной безопасности позволяет успешно внедрять полученный опыт не только на государственном уровне, но и на региональном. В этом кроется существенное отличие от иранской политики – Саудовская Аравия является единственным актором исламского мира, стремящимся к созданию единых выработанных подходов к обеспечению кибербезопасности. Таковым является Совет сотрудничества арабских государств Персидского залива [11] – институциональная структура, которая продвигает понимание информационной безопасности, характерное для западной литературы. Именно данный аспект и является камнем преткновения с другими странами ближневосточного пространства.

Как и в случае с Ираном, движущей силой стремительного развития в области цифровой безопасности стали неоднократные хакерские атаки со стороны йеменских хакеров на Королевство, в частности, из-за вмешательства последнего во внутренние дела Йемена.

Кроме того, Саудовская Аравия активно внедряет цифровые технологии, трансформируя все основные сферы жизнедеятельности общества, будь то здравоохранение, образование или сфера туризма. В Королевстве разработаны и эффективно действуют ряд систем, позволяющих сократить лишние расходы.

Израиль

Израиль невозможно назвать приверженцем проводимой политики Саудовской Аравии на Ближнем Востоке. Тем не менее, напряженность в отношениях с Ираном ставит этих акторов на одну сторону. Процесс унификации подходов к обеспечению региональной безопасности в этом регионе происходил за счет подписания в 2020 году «Авраамских соглашений». Тем не менее, существенное влияние на дальнейшее сотрудничество в данной области оказывает палестино-израильский конфликт, в частности, беспорядочные атаки на гражданское население со стороны Израиля. Кроме того, страны, состоящие в Совете сотрудничества арабских государств Персидского залива, связаны рядом договоров на поставку израильского программного обеспечения для обеспечения кибербезопасности.

Стоит отметить, что система кибербезопасности самого Израиля имеет глубокую разветвленную структуру, которая включает в себя большое количество кибергруппировок, так или иначе связанных с государственными органами. В свою очередь, данный факт позволяет Израилю продвигать собственную модель обеспечения безопасности в информационном пространстве. Ряд стран, состоящих в Совете сотрудничества арабских государств Персидского залива, связаны договорами на поставку израильского программного обеспечения для обеспечения кибербезопасности [12]. Особый интерес в этой связи представляет политика Катара, который, с одной стороны, выступает союзником Саудовской Аравии в рамках палестинского вопроса, но в то же время ведет активное непубличное сотрудничество с Израилем в области кибербезопасности. Такие израильские компании, как ClearSky и Cyber Security [13], активно способствовали построению кибербезопасности в Катаре, а также неоднократно отражали множественные кибератаки со стороны других региональных акторов, в частности Ирана.

Другим примером тесного взаимодействия на просторах ближневосточного региона в области кибербезопасности является внедрение Саудовской Аравией технологий искусственного интеллекта, предоставляемых компанией IntuView, в целях контроля и предотвращения террористических угроз.

Турция

Учитывая геополитическое положение Турции, а также проходящую по её территории инфраструктуру для транспортировки газа, ближневосточное государство является безоговорочным претендентом на региональное лидерство. В этой связи обеспечение региональной кибербезопасности соответствует их национальным интересам, при этом их политика скорее находится в оппозиции к странам, входящим в Совет сотрудничества арабских государств Персидского залива, и, в частности, к Саудовской Аравии. На официальном уровне соответствующими доктринами закреплено наличие киберподразделений Türk Siber Ordusu [10]. В то же время, как и Саудовская Аравия, Турция в большей степени перенимает опыт западных коллег посредством консультаций, а также активного участия в различных киберучениях международного уровня. Тем не менее, несмотря на разницу в подходах к обеспечению информационной безопасности, со странами Персидского залива Турция выстраивает такую линию поведения, которая способствует поиску взаимодополняющих решений в этом направлении.

Кроме того, помимо вышеупомянутых государственных акторов, обладающих специализированными подразделениями, на ближневосточном пространстве также действуют и негосударственные элементы, которые своим присутствием вносят деструктивный элемент в развитие, пусть и разных подходов. Как правило, это различные террористические ячейки, которые также прибегают к использованию информационных технологий. Одной из наиболее активных является «Объединённый киберхалифат ИГИЛ» (признан террористической организацией на

территории Российской Федерации), занимающийся промышленным шпионажем, но при этом способный осуществлять масштабные кибератаки.

Заключение

Исходя из вышесказанного, наличие как внутренних, так и внешних препятствий и угроз ставит перед государствами Ближнего Востока необходимость унификации и выработки общих подходов к обеспечению кибербезопасности на региональном уровне. Последовательная политика приводит к сближению и развитию сотрудничества в рамках всего Ближнего Востока, несмотря на наличие диаметрально противоположных решений в области цифровой безопасности. Кроме того, существующие организации, которые создавались как военные коалиции, постепенно внедряют и информационную составляющую в целях обеспечения защиты региона в цифровом пространстве [11]. В частности, в рамках Совета сотрудничества арабских государств Персидского залива действует военная составляющая Совета под названием «Щит полуострова», которая изначально создавалась для противодействия и нейтрализации агрессии против любого участника организации. По мере внедрения информационных технологий традиционным методам противодействия добавились меры в киберпространстве. На данный момент успешно разработана и функционирует система по противодействию возникающим киберугрозам в рамках ССАГПЗ, что представляет собой важнейшую составляющую интеграционных процессов ближневосточного региона.

Кроме того, важным решением на пути становления единой системы коллективной кибербезопасности между странами-участниками Совета сотрудничества арабских государств Персидского залива является внедрение программ «Видение-2030», призванных установить общерегиональные стратегии по диверсификации экономик и переходу от традиционного для этого региона экспорта полезных ископаемых. При этом цифровизации отводится ключевое место для дальнейшего экономического развития Ближнего Востока во всех отраслях. Лидером по реализации данной программы является Саудовская Аравия, которая ещё с 2016 года начала стремительную диверсификацию экономики, причиной которой стал экономический кризис в Королевстве из-за обвала цен на нефть [15].

Таким образом, несмотря на наличие существенных проблем, к которым относятся конкуренция и продвижение собственных интересов в области цифрового развития и обеспечения безопасности, грозящие углублением противоречий между ближневосточными государствами, вмешательство внерегиональных акторов, в числе которых можно выделить США, ряд развитых стран Европы, Китай, стремящихся обеспечить каждый свои собственные интересы в данном регионе, наличие внесистемных элементов в виде террористических ячеек, конкуренция в области кибербезопасности представляет собой движущую силу качественного преображения ближневосточного региона.

Конкурирующие за лидерство региональные державы так или иначе согласуют свою политику в области обеспечения кибербезопасности в части совместного противостояния как региональным, так и внерегиональным угрозам, что проявляется в закреплении институционализированных структур на основе существующих интеграционных объединений, а также в совместном нивелировании киберугроз. Несмотря на отсутствие политической стабильности на Ближнем Востоке, уже сейчас прослеживается переход интеграции стран Ближнего Востока в цифровой сфере в экономическую и политическую составляющую. Это видно на примере взаимодействия Саудовской Аравии и Израиля, Ирана и Катара, а также взаимодействия между другими региональными акторами.

Однако существенные достижения в области сотрудничества между государствами Ближнего Востока окончательно подорваны действиями израильского правительства. Расширение палестино-израильского конфликта затронуло и близлежащие страны. В частности, последняя кибератака, проведённая Израилем на территории Ливана, привела к многочисленным жертвам, в том числе и среди гражданского населения. Тем самым Израиль открыл «ящик Пандоры» в области обеспечения кибербезопасности в глобальном масштабе.

Литература

1. Валиахметова Г.Н. Исламский мир в условиях цифровых угроз XXI века // MINBAR. Islamic studies. 2019. Т. 12. № 1. С. 95-110
2. Гайворонская Я. В., Мирошниченко О. И. Правовые проблемы цифровизации: теоретико-правовой аспект // Правовая парадигма. 2019. № 18 (4). С. 27.
3. Герасимова Т. А., Москвитина Н. В. Содержание понятий «цифровая экономика» и «цифровизация в сфере государственного управления» // Социальная реальность виртуального пространства: материалы I Междунар. науч.-практ. конф. Иркутск: ИГУ, 2019. С. 310–315
4. Кильченко В.С. Политика Исламской Республики Иран в сфере информационной безопасности // Сборник XIII Международной научно-практической конференции студентов, магистрантов, аспирантов, соискателей. Саратовский национальный исследовательский государственный университет имени Н.Г. Чернышевского. 2020. С. 91-93.
5. Концепция стратегии кибербезопасности Российской Федерации. [Электронный ресурс]. URL: http://council.gov.ru/media/files/41d4b3dfbdb25cea8a73.pdf (дата обращения 01.10.2024)
6. Кортунов А.В. Будущее Ближнего Востока: два горизонта угроз и возможностей // РСМД. 2019. URL: https://russiancouncil.ru/ analytics-and-comments/analytics/budushchee-blizhnego-vostoka-dva-gorizonta-ugroz-i-vozmozhnostey/ (дата обращения: 13.07.2024)
7. Кузнецова Т.Ф. Цифровизация как культурная ценность и цифровые технологии // Горизонты гуманитарного знания. № 5, 2019, с. 3-13.
8. Науменко Т.В., Тимахов К.В. Саудовская Аравия и её конкурентоспособность среди стран ближневосточного региона // Вестник МГИМО-Университета. 2019. 1(64). С. 147-167
9. Талеб Н. Черный лебедь. Под знаком непредсказуемости // М. - 2009. – 528 с.
10. Турецкая киберармия: эра электронных янычаров // ПИР-Центр. 2020. [Электронный ресурс]. URL: http://www.pircenter.org/blog/view/id/426 (дата обращения: 13.07.2024).
11. Цуканов Л.В. Силы безопасности ССАГПЗ: цифровое измерение // Российский Совет по международным делам. 28.07.2021. [Электронный ресурс]. URL: https://russiancouncil.ru/analytics-and-comments/columns/middle-east/silybezopasnosti-ssagpz-tsifrovoe-izmerenie (дата обращения: 13.07.2024).
12. Цуканов Л.В. Цифровые химеры Персидского залива: кто займет место Ирана? // Российский Совет по международным делам. 22.02.2022. [Электронный ресурс]. URL: https://clck.ru/eJdYR (дата обращения: 01.10.2022).
13. Цуканов Л.В. Сотрудничество Израиля и Катара в сфере кибербезопасности // Теории и проблемы политических исследований. 2021. Т. 10. № 5А. С. 28-36.
14. Global Cybersecurity Index 2020 // ITU Publications. 2022. [Электронный ресурс]. URL: https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E/ (дата обращения: 14.07.2024).
15. How Prepared is Saudi Arabia for a Cyber War? // Institute for National Security Studies. 2019. [Электронный ресурс]. URL: https://www.inss.org.il/publication/howprepared-is-saudi-arabia-for-a-cyber-war/ (дата обращения: 27.09.2024)
16. Middle East Cybersecurity Market by Offering (Solutions and Services), Solution Type, Security Type, Deployment Mode (On-Premises, Cloud, Hybrid), Organization Size (Large Enterprises, SME), Vertical and Region - Forecast to 2028 [Электронный ресурс]. URL: https://www.researchandmarkets.com/report/middle-east-it-security-market (дата обращения: 13.07.2024)
17. National cyber security index. [Электронный ресурс]. URL: https://ncsi.ega.ee/compare/ (дата обращения: 14.07.2024)

18. Semantic Scholar. [Электронный ресурс]. URL: https://www.semanticscholar.org/paper/Digital-Strategy-and-Digital-TransformationGobble/0f9d211b9ebab742b348a8800d04ab44b57353dd
19. Vision 2030. [Электронный ресурс]. URL: https://www.vision2030.gov.sa/ (дата обращения: 14.07.2024).

KEY CYBER SECURITY CHALLENGES IN THE MIDDLE EAST

Emelin, Danil R.

Lomonosov Moscow State University, Faculty of global processes, graduate student
Moscow Russian Federation
danil.emelin@mail.ru

Abstract

With the development of information technology, cybersecurity has become of paramount importance for maintaining the stability of political processes taking place in the international arena. Conflicts between states have moved to a completely new dimension – information. At the same time, ensuring the security of the information space and the development of relevant institutional structures vary from region to region. In this regard, the Middle East, being one of the most unstable regions in the world, faces unique challenges in the field of cybersecurity, which are manifested in both the economic and geopolitical essence of international processes. The author examines the main problems, as well as approaches to implementing policies in the field of cybersecurity in the countries of the Middle East region.

Keywords

Middle East, cybersecurity, information society, globalization, regional security, cyberterrorism

References

1. Valiahmetova G.N. Islamskij mir v usloviyah cifrovyh ugroz HKHI veka // MINBAR. Islamic studies. 2019. T. 12. № 1. S. 95-110
2. Gajvoronskaya YA. V., Miroshnichenko O. I. Pravovye problemy cifrovizacii: teoretiko-pravovoj aspekt // Pravovaya paradigma. 2019. № 18 (4). S. 27.
3. Gerasimova T. A., Moskvitina N. V. Soderzhanie ponyatij «cifrovaya ekonomika» i «cifrovizaciya v sfere gosudarstvennogo upravleniya» // Social'naya real'nost' virtual'nogo prostranstva: materialy I Mezhdunar. nauch.-prakt. konf. Irkutsk: IGU, 2019. S. 310–315
4. Kilchenko V.S. Politika Islamskoj Respubliki Iran v sfere informacionnoj bezopasnosti // Sbornik XIII Mezhdunarodnoj nauchno-prakticheskoj konferencii studentov, magistrantov, aspirantov, soiskatelej. Saratovskij nacional'nyj issledovatel'skij gosudarstvennyj universitet imeni N.G. CHernyshevskogo. 2020. S. 91-93.
5. Koncepciya strategii kiberbezopasnosti Rossijskoj Federacii. [Elektronnyj resurs]. URL: http://council.gov.ru/media/files/41d4b3dfbdb25cea8a73.pdf (data obrashcheniya 01.10.2024)
6. Kortunov A.V. Budushchee Blizhnego Vostoka: dva gorizonta ugroz i vozmozhnostej // RSMD. 2019. URL: https://russiancouncil.ru/ analytics-and-comments/analytics/budushchee-blizhnego-vostoka-dva-gorizonta-ugroz-i-vozmozhnostey/ (data obrashcheniya: 13.07.2024)
7. Kuznecova T.F. Cifrovizaciya kak kul'turnaya cennost' i cifrovye tekhnologii // Gorizonty gumanitarnogo znaniya. № 5, 2019, s. 3-13.
8. Naumenko T.V., Timahov K.V. Saudovskaya Araviya i eyo konkurentosposobnost' sredi stran blizhnevostochnogo regiona // Vestnik MGIMO-Universiteta. 2019. 1(64). S. 147-167
9. Taleb N. CHernyj lebed'. Pod znakom nepredskazuemosti // M. - 2009. – 528 s.
10. Tureckaya kiberarmiya: era elektronnyh yanycharov // PIR-Centr. 2020. [Elektronnyj resurs]. URL: http://www.pircenter.org/blog/view/id/426 (data obrashcheniya: 13.07.2024).
11. Cukanov L.V. Sily bezopasnosti SSAGPZ: cifrovoe izmerenie // Rossijskij Sovet po mezhdunarodnym delam. 28.07.2021. [Elektronnyj resurs]. URL: https://russiancouncil.ru/analytics-and-comments/columns/middle-east/silybezopasnosti-ssagpz-tsifrovoe-izmerenie (data obrashcheniya: 13.07.2024).
12. Cukanov L.V. Cifrovye himery Persidskogo zaliva: kto zajmet mesto Irana? // Rossijskij Sovet po mezhdunarodnym delam. 22.02.2022. [Elektronnyj resurs]. URL: https://clck.ru/eJdYR (data obrashcheniya: 01.10.2022).
13. Cukanov L.V. Sotrudnichestvo Izrailya i Katara v sfere kiberbezopasnosti // Teorii i problemy politicheskih issledovanij. 2021. T. 10. № 5A. S. 28-36.

14. Global Cybersecurity Index 2020 // ITU Publications. 2022. [Elektronnyj resurs]. URL: https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E/ (data obrashcheniya: 14.07.2024).
15. How Prepared is Saudi Arabia for a Cyber War? // Institute for National Security Studies. 2019. [Elektronnyj resurs]. URL: https://www.inss.org.il/publication/howprepared-is-saudi-arabia-for-a-cyber-war/ (data obrashcheniya: 27.09.2024)
16. Middle East Cybersecurity Market by Offering (Solutions and Services), Solution Type, Security Type, Deployment Mode (On-Premises, Cloud, Hybrid), Organization Size (Large Enterprises, SME), Vertical and Region - Forecast to 2028 [Elektronnyj resurs]. URL: https://www.researchandmarkets.com/report/middle-east-it-security-market (data obrashcheniya: 13.07.2024)
17. National cyber security index. [Elektronnyj resurs]. URL: https://ncsi.ega.ee/compare/ (data obrashcheniya: 14.07.2024)
18. Semantic Scholar. [Elektronnyj resurs]. URL: https://www.semanticscholar.org/paper/Digital-Strategy-and-Digital-TransformationGobble/0f9d211b9ebab742b348a8800d04ab44b57353dd
19. Vision 2030. [Elektronnyj resurs]. URL: https://www.vision2030.gov.sa/ (data obrashcheniya: 14.07.2024).