УДК 341.171

Э.В. Горян

Владивостокский государственный университет экономики и сервиса
Владивосток. Россия

Ведущая роль Сингапура в обеспечении кибербезопасности в АСЕАН: промежуточные результаты и перспективы дальнейшего расширения

В международном праве отсутствует универсальный правовой механизм обеспечения кибербезопасности. Одна из причин видится в различии в подходах к защите CII, а также в разном уровне информационно-технологического развития государств. Но постепенно более развитые в этом плане государства проявляют инициативу регионального сотрудничества в сфере кибербезопасности, предлагая действующие и опробованные на национальном уровне модели. Как правило, инициаторами выступают социально и экономически развитые государства региона. В АСЕАН таким бесспорным лидером является Сингапур. Предмет исследования составляют основные нормативно-правовые акты в сфере обеспечения кибербезопасности Сингапура, региональные и международные инициативы этого государства, а также ряд научных исследований по теме.

С целью получения наиболее достоверных научных результатов будет использован ряд общенаучных (системно-структурный, формально-логический и герменевтический) и специальных юридических методов познания (сравнительно-правовой и формально-юридический). Использование этих методов имеет комплексный характер.

Национальный правовой механизм кибербезопасности Сингапура имеет самую длительную по сравнению с другими государствами-участниками АСЕАН историю становления. Это обусловлено темпами социально-экономического развития государства, его фактическим статусом регионального и международного торгово-экономического центра. Сингапур реализует модель публично-частного партнерства обеспечения кибербезопасности, где государству отведена роль политико-направляющего субъекта (например, при определении секторов CII), мнение представителей частного сектора играет решающую роль при определении содержания нормативного механизма кибербезопасности, а сами они включены в институционный механизм обеспечения кибербезопасности. Законодатель смог найти баланс в обеспечении публичных интересов и защите гражданских прав и свобод, что очень важно в условиях сохранения и увеличения инвестиционной привлекательности государства. Определение регионального и международного сотрудничества в качестве одной из четырех опор стратегии кибербезопасности и запуск ряда успешных проектов в этой сфере делают Сингапур лидером не только в АСЕАН, но и на международной арене. На наш взгляд, сохранение текущего status quo, а в перспективе – дальнейшее развитие этого направления внешней политики Сингапура способны вывести это государство на ведущие позиции при разработке универсального международно-правового механизма обеспечения кибербезопасности.

Ключевые слова и словосочетания: кибербезопасность, АСЕАН, Сингапур, ключевая информационная инфраструктура, международный механизм.

Горян Элла Владимировна – канд. юрид. наук, доцент кафедры гражданско-правовых дисциплин Института права, доцент; e-mail: ella.goryan@vvsu.ru.

E.V. Gorian
Vladivostok State University of Economics and Service
Vladivostok. Russia

Singapore's leadership on cybersecurity in ASEAN: intermediate results and future prospects

There is no any universal legal mechanism for cyberprotection in international law. The difference in approaches to the protection of CII, as well as different levels of states' information and technological development are the reasons of it. But the most developed states are taking the initiative of providing the regional cooperation in the field of cybersecurity by offering models which proved their validity at the national level. Usually the initiators are the most socially and economically developed states of the region. Singapore is such an indisputable leader in ASEAN. The subject of the study are the main regulatory acts in the sphere of cybersecurity in Singapore, regional and international initiatives of this state, as well as a numerous of researches on the topic.

In order to obtain the most reliable scientific results, a number of general scientific (system-structural, formal-logical and hermeneutic methods) and special legal methods of cognition (comparative legal and formal-legal methods) will be used. The use of these methods is complex.

Singapore's national legal cybersecurity mechanism has the longest history of development among other ASEAN member states. This can be explained by pace of socio-economic development of the state and by its actual status as a regional and international trade and economic center. Singapore implements the public-private partnership model for cybersecurity, where the state is assigned the role of politically-directing entity (for example, in the definition of CII sectors), the opinions of stakeholders from the private sector play a decisive role in determining the content of the regulatory mechanism for cybersecurity. Stakeholders are also included in the institutional mechanism for ensuring cybersecurity. The legislator managed to find a balance in securing public interests and protecting civil rights and freedoms, which is very important in the conditions of sustaining the investment attractiveness of the state. The emphasizing of regional and international cooperation as one of the four pillars of the cybersecurity strategy and the launch of a number of successful projects in this sphere makes Singapore a leader not only in ASEAN, but also in the international arena. The retention of the current status quo, and in the future - the further development of this aspect of Singapore's foreign policy will help to gain the leading position in the law-making process of a universal international legal mechanism for cyberprotection.

Keywords: cybersecurity, ASEAN, Singapore, critical information infrastructure, international mechanism.

Актуальность темы исследования

В последние годы в государствах Юго-Восточной Азии наблюдается резкий рост цифровой экономики (digital economy). В своем отчете «e-Conomy SEA Spotlight 2017: Unprecedented growth for Southeast Asia's $50B internet economy» аналитики Google и Temasek оценили рынок цифровой экономики региона в 2017 году в 50 млрд долларов США, что превзошло все ожидания экспертов [15]. В частности, к концу 2017 года количество интернет-пользователей составило более 330 млн человек, показав рост на 70% по сравнению с 2015 годом. Более 90% таких пользователей используют смартфоны для выхода в интернет и тратят около 3,6 часов в день на мобильный интернет, что гораздо больше по сравнению с пользователями из других регионов. Такой резкий рост цифровой экономики Юго-Восточной Азии связывают с успехами шести компаний, каждая из которых оценивается приблизительно в 1 млрд долларов США: 1) Grab Holdings – разработчик транспортных мобильных приложений Grab Taxi, GrabCar, GrabBike, GrabExpress, используемых

во всех странах Юго-Восточной Азии; 2) Traveloka – лидер бронирования гостиниц и авиабилетов; 3) Tokopedia – ведущая платформа электронной торговли в Инденезии; 4) Go-Jek – многопрофильное мобильное приложение (транспорт, доставка еды, перевозки, платежи, разнообразные услуги); 5) SEA Group – платформа электронной торговли, цифровых развлечений, электронных платежей; 6) Lazada – ведущая платформа электронной торговли в Юго-Восточной Азии. Рост цифровой экономики связан преимущественно с развитием четырех основных отраслей: 1) бронирование гостиниц и авиабилетов (26,6 млрд долларов США в 2017 году, что демонстрирует рост 18% по сравнению с 2015 годом); 2) онлайн-СМИ (6,9 млрд долларов США в 2017 году, рост по сравнению с 2015 годом составил 36%); 3) электронная торговля (11 млрд. долларов США с увеличением объема операций на 41% по сравнению с 2015 годом); 4) транспортные услуги (5 млрд долларов США и рост на 100% по сравнению с 2015 годом) [15].

Такие впечатляющие темпы роста цифровой экономики в Юго-Восточной Азии обусловливают необходимость гармонизации законодательства государств-участников Ассоциации государств Юго-Восточной Азии (далее – АСЕАН). Пять участников АСЕАН (Вьетнам, Индонезия, Малайзия, Сингапур, Таиланд) уже присоединились к так называемому Единому окну АСЕАН (ASEAN Single Window) – онлайн-платформе для ускоренного таможенного оформления посредством электронного обмена торговыми документами проведения трансграничных операций. На очереди – гармонизация правил электронной торговли, норм защиты прав потребителей, защиты персональных данных, антимонопольной политики и кибербезопасности, разработка правовой основы разрешения споров в интернете [19]. Среди государств-участников АСЕАН ключевая роль в интеграционных процессах по праву принадлежит Сингапуру. Будучи самым развитым с точки зрения информационных технологий в мире государством, Сингапур является также ключевым международным финансовым и торговым центром. Это делает его идеальной мишенью для кибератак, последствия которых гораздо серьезнее, чем обычное нарушение общественного и экономического благополучия Сингапура – под удар попадает вся цепочка международных поставок и банковская сфера, а в перспективе – международная экономика. Поэтому в 2016 году в Сингапуре была разработана одна из лучших на сегодняшний день национальных стратегий кибербезопасности (National Cybersecurity Strategy 2016, далее – NCS), а в 2018 году Парламент Сингапура принял Акт о кибербезопасности (Cybersecurity Act 2018, далее – CSA), который считается стандартом нового поколения для защиты ключевой информационной инфраструктуры (Critical Information Infrastructure, далее – CII), что делает его объектом пристального внимания профессионалов из разных сфер.

В 2018 году на 32-м ежегодном саммите государств-участников АСЕАН в Сингапуре, который в этом году председательствует в Ассоциации государств Юго-Восточной Азии, была обозначена повестка сотрудничества на год. В частности, был акцентирован такой ключевой аспект сотрудничества, как кибербезопасность, что связано с возросшим характером и масштабом кибератак. В своем заявлении главы государств-участников АСЕАН обратились к соответствующим профильным минис-

трам по поводу необходимости рассмотрения всех возможных путей координации политики кибербезопасности, дипломатии и технического сотрудничества на разных уровнях трех опор АСЕАН: Сообщества политической безопасности АСЕАН (ASEAN Political-Security Community, APSC), Экономического сообщества АСЕАН (ASEAN Economic Community, AEC) и Социокультурного сообщества АСЕАН (ASEAN Socio-Cultural Community, ASCC). Этот вопрос также должен стать предметом обсуждений на предстоящей Министерской конференции АСЕАН по кибербезопасности (ASEAN Ministerial Conference on Cybersecurity, AMCC) и совещании министров по телекоммуникациям и информационным технологиям (ASEAN Telecommunications and Information Technology Ministers' Meeting, TELMIN), а также на соответствующих секционных заседаниях Министерского совещания АСЕАН по вопросам транснациональной преступности (ASEAN Ministerial Meeting on Transnational Crime, AMMTC) с целью определения конкретного списка практических действий государств-участников АСЕАН в сфере кибербезопасности (защита личных данных и сотрудничество в киберпространстве). Главы государств-участников АСЕАН признали эффективность инициированной в 2016 году Сингапуром Программы АСЕАН по увеличению киберпотенциала (ASEAN Cyber Capacity Programme) (п. 6) [9]. Поэтому изучение опыта Сингапура по обеспечению кибербезопасности на национальном и региональном уровнях необходимо как для совершенствования российского механизма кибербезопасности, так и для определения стратегии и тактики выхода российских компаний на международные рынки Юго-Восточной Азии. Все вышесказанное свидетельствует об актуальности темы исследования.

Постановка проблемы исследования

Коммуникационные сети являются основой информационного общества и важной частью единого цифрового рынка. Некоторые из них имеют критически важное значение из соображений национальной безопасности, поскольку они обеспечивают жизненно важные ресурсы или поддерживают их функционирование. Такие коммуникационные сети имеют решающее значение для удобства и даже существования людей [8], поэтому они определяются как ключевая информационная инфраструктура (CII). CII – это основная цель кибератак, поэтому государства пытаются противодействовать им путем создания адекватных механизмов, которые могли бы оптимально защитить CII при соблюдении основных гражданских прав [20]. В целом ситуация с защитой CII на национальном уровне удовлетворительная. Можно наблюдать основную тенденцию делегирования полномочий специальным органам кибербезопасности, ведомствам по чрезвычайным ситуациям или другим национальным регулирующим органам, отвечающим за выполнение оперативных задач. Многие из этих органов несут ответственность за выполнение дополнительных задач на стратегическом или политическом уровне, таких, как разработка стратегических документов, контроль над национальной группой реагирования на инциденты в области компьютерной безопасности или разработка законодательства. Тем не менее, значительная часть государств включила в институциональный механизм кибербезопасности представителей частного сектора, поскольку именно они несут ответственность за обеспечение

устойчивости коммуникационных сетей и принимают участие в обеспечении национальной информационной безопасности, выполняя технические экспертные знания [17]. Для всех государств важнейшими секторами CII, в отношении которых предусмотрено самое строгое нормативное регулирование в сфере кибербезопасности, являются телекоммуникационный, финансовый и энергетический. Однако не все из государств проводят оценку риска на национальном уровне. Как правило, они осуществляют политику возложения ответственности за оценку риска на отраслевые агентства или отдельных операторов [21, с. 9]. Поэтому национальные стандарты кибербезопасности варьируются от простейших до самых передовых. Именно те государства, которые играют ведущую роль в международных экономических отношениях и на цифровых рынках, постоянно развивают свои национальные стандарты защиты CII для обеспечения не только внутреннего взаимодействия между бизнесом и обществом, но и глобальной цепочки поставок. Поиск баланса между публичными и частными интересами – ключевая проблема при разработке механизма кибербезопасности.

В международном праве пока отсутствует правовой механизм обеспечения кибербезопасности. К причинам относятся различие в подходах к защите CII, а также разный уровень информационно-технологического развития государств. Но постепенно более развитые в этом плане государства проявляют инициативу регионального сотрудничества в сфере кибербезопасности, предлагая действующие и опробованные на национальном уровне модели. Как правило, инициаторами выступают социально и экономически развитые государства региона. В АСЕАН таким бесспорным лидером является Сингапур.

Научная гипотеза

Сингапур является первым государством Юго-Восточной Азии, которое модернизировало свое законодательство в сфере кибербезопасности, возложив на частный сектор обязанности по обеспечению защиты компьютерных систем. Предложенная Сингапуром модель обеспечения кибербезопасности CII является на сегодняшний день наиболее сбалансированной с точки зрения публичных и частных интересов, что объясняет ведущую роль этого государства в обеспечении кибербезопасности в АСЕАН.

Цели и задачи исследования

Цель нашего исследования – охарактеризовать модель обеспечения кибербезопасности CII в Сингапуре, которая определяет его роль в гарантировании кибербезопасности АСЕАН. Задачи исследования заключаются в исследовании основных положений Стратегии кибербезопасности Сингапура 2016 года, Акта о кибербезопасности 2018 года и Программы АСЕАН по увеличению киберпотенциала 2017 года, предложенной Сингапуром.

Методология

С целью получения наиболее достоверных научных результатов будет использован ряд общенаучных (системно-структурный, формально-логический и герменевтический) и специальных юридических методов познания (сравнительно-правовой и формально-юридический). Применение этих методов носит комплексный характер.

Предмет исследования, источниковая база исследования, противоречия в имеющихся исследованиях и авторская позиция

Предмет исследования составляют основные нормативно-правовые акты в сфере обеспечения кибербезопасности Сингапура, региональные и международные инициативы этого государства, а также ряд научных исследований по теме.

Выбранная нами для исследования тема мало представлена в российской научной литературе. Вопросы сотрудничества Российской Федерации с АСЕАН рассматриваются в работах С.Н. Курского [4] и Д.Г. Фатуллаева [6]. Аспект интеграционных процессов в АСЕАН представлен в работах А.А. Савельева [5] и Г.М. Костюниной [2; 3]. Роль Сингапура в развитии интеграционных процессов в АСЕАН исследовала Э.М. Гуревич [1]. Вопросы обеспечения кибербезопасности в государствах-участниках АСЕАН и в рамках АСЕАН в отечественной литературе не рассматриваются вообще.

В зарубежной научной литературе исследуемая тема является предметом активных дискуссий. В частности, авторы отмечают неоднозначность использования государствами частного сектора для обеспечения безопасности CII, хотя они эксплуатируются частными организациями, которые на международном уровне участвуют во всей глобальной цепочке поставок. Благодаря своему оперативному потенциалу частный сектор привлекается как эксперт в области безопасности сетевых и информационных систем, знания которого имеют решающее значение для регулирования деятельности на местах. Б. Фарранд и Х. Каррапико отмечают постепенно меняющуюся роль частного сектора в защите CII от одной из жертв, нуждающихся в защите на первом этапе, к коммерческому субъекту, несущему ответственность за обеспечение устойчивости сети на втором этапе, до активного разработчика политики на третьем этапе путем участия в регулировании национальной информационной системы путем предоставления технической экспертизы [17]. Каждое государство разрабатывает собственную модель защиты CII (в первую очередь, физической), используя соответствующие методологические подходы для оценивания угроз для объектов инфраструктуры. Д. Бобро подчеркивает необходимость учета всех опасностей (любого происхождения и направленности). Предложенная им модель угроз (threat model) учитывает не только характеристики нарушителя, но и характеристики объекта и социально-политической ситуации [7]. Характер киберпространства и его постоянная эволюция являются ключевыми факторами развития адекватных национальных механизмов обеспечения кибербезопасности. В частности, израильские исследователи обосновывают необходимость эволюции правительственных структур на современном этапе путем формирования единого гражданского ведомства с конкретными оперативными возможностями, отвечающего за защиту национального киберпространства и реализующего полномочия по обеспечению кибербезопасности [20]. Как видно из изложенного, исследователи придерживаются точки зрения о необходимости активного привлечения частного сектора в деятельность институционального механизма кибербезопасности, а также о многофакторном подходе к оценке киберрисков. На наш взгляд, такой подход оправдан и позволяет создать прозрачный, сбалансированный и координи-

руемый с учетом новейших технологических знаний механизм противодействия кибервмешательствам.

Основная часть

В международном праве однозначное определение ключевой информационной инфраструктуры (CII) отсутствует. Например, Европейская комиссия в своей Директиве 2008/114/ЕС определяет CII как систему информационно-коммуникационных технологий, которые являются важными инфраструктурами сами по себе или необходимы для функционирования ключевых инфраструктур (телекоммуникации, компьютеры, программное обеспечение, Интернет, спутники и т. д.) [10]. В «Зеленой книге» Европейской программы защиты критической инфраструктуры Европейская комиссия определяет примерный список из 11 важнейших секторов: энергетика, информационно-коммуникационные технологии, водоснабжение, продовольствие, здравоохранение, финансы, общественный порядок и безопасность, гражданская администрация, транспорт, химическая и ядерная промышленность, космос и исследования [18].

Поэтому каждое государство устанавливает критерии для определения любых данных, баз данных, сетей, телекоммуникационной инфраструктуры (или ее части) как CII. Некоторые государства уже определили свои секторы CII и приступили к этапу обеспечения их безопасности, в то время как другие только приступают к этапу определения [21, с. 7]. Это приводит к различию в национальных механизмах защиты CII в зависимости от информационных активов, полномочий властей, методов регулирования и проч. Например, государства-члены ЕС определяют свои собственные секторы CII, исходя из своих особенностей: Австрия из предложенного Еврокомиссией списка исключила химическую и ядерную промышленность, Франция исключила химическую и ядерную промышленность, но включила промышленность как отдельный сектор; Италия и Греция исключили почти все секторы за исключением энергетики и транспорта; Великобритания исключила общественный порядок, химическую и ядерную промышленность, космос и исследования, но включила службы экстренной помощи [21, с. 5].

Специалисты в сфере кибербезопасности определяют четыре уровня обеспечения государствами безопасности CII. Первый уровень характеризуется отсутствием действий, связанных с защитой CII; государства определили только транспорт и энергию в качестве важнейших секторов. На втором уровне государство определяет сектор информационно-коммуникационных технологий как один из важнейших секторов, которые необходимо защитить. На третьем уровне государства разрабатывают общую методологическую основу для определения важнейших информационных активов с конкретными шагами и обязанностями, возложенными на заинтересованные стороны. И на самом высоком уровне обеспечения, четвертом, государство разрабатывает определение и устанавливает конкретные критерии идентификации CII. Это свидетельствует о принятии конкретных мер для идентификации и защиты CII государством [21, с. 6]. Важнейшим фактором защиты CII является эффективное сотрудничество между государственным сектором (государственными и уполномоченными агентствами) и частным сектором,

который часто контролирует CII. Общепринятой практикой выступает то, что поставщики услуг определяются уполномоченным агентством как операторы CII: они предлагают конкретные ключевые услуги для общества, охватывают большой объем населения и территории, их риски могут стать национальными [21, с. 16].

Как правило, государства определяют секторы CII и ключевые факторы их защиты в соответствующих стратегиях и закрепляют механизм обеспечения кибербезопасности в специальном законе. В государствах-участниках АСЕАН ситуация с нормативным обеспечением выглядит следующим образом.

Во Вьетнаме до июня 2018 года отсутствовал какой-либо нормативно-правовой акт, посвященный кибербезопасности. 1 января 2019 года вступит в силу принятый в июне 2018 года закон о кибербезопасности, который международные правозащитные организации и ассоциации предпринимателей уже назвали угрозой гражданским и экономическим свободам [22].

В Индонезии законодательство о кибербезопасности находится в стадии формирования (разрабатывается проект закона об информационных технологиях и электронных транзакциях – Law on Information Technology and Electronic Transaction, ITET). В данный момент действует закон от 2008 года в редакции от 2016 года об информации и электронных транзакциях (Law on Information and Electronic Transaction), имеющий множество пробелов и не справляющийся с современными киберугрозами [13].

В Малайзии действует второй старейший среди государств-участников АСЕАН Акт о компьютерных преступлениях (Computer Crime Act 1997). Среди других специальных законов следует отметить Акт о защите персональных данных (Personal Data Protection Act 2010), в 2016 году вступила в действие Политика национальной кибербезопасности (National Cybersecurity Policy 2016), в которой было дано определение секторов CII, год спустя был начат процесс по разработке закона о кибербезопасности.

Таиланд является одним из двадцати государств мира, занимающих лидирующие позиции в обеспечении кибербезопасности [26]. Уже более десяти лет в стране действует Акт о компьютерных преступлениях (Computer Crimes Act 2007 в редакции 2017 года), Акт о защите персональных данных (Personal Data Protection Act 2018), в настоящее время проходят слушания по поводу утверждения Билля о национальной кибербезопасности (National Cybersecurity Bill) и национальной стратегии кибербезопасности.

В 2017 году в Филиппинах начал реализовываться План национальной кибербезопасности 2022 (National Cybersecurity Plan 2022), в котором были определены секторы CII. С 2012 года действуют Акт о предотвращении киберпреступности (Cybercrime Prevention Act 2012) и Акт о персональных данных (Data Privacy Act 2012).

В других государствах АСЕАН (Бруней-Даруссалам, Камбоджа, Лаос, Мьянма) отсутствуют разработанные национальные стратегии кибербезопасности и соответствующее законодательство (за исключением Лаоса, приступившего к разработке пакета законов о киберпреступности).

Сингапур стал первым государством в АСЕАН, принявшим в 1993 году Акт о злоупотреблениях в компьютерных сетях и кибербезопасности (Computer Misuse

and Cybersecurity Act 1993 в редакции 2017 года). Сегодня законодательство этого государства в сфере кибербезопасности представлено Актом о защите персональных данных 2012 года (Personal Data Protection Act 2012), Национальным планом действий в отношении киберпреступности 2016 года (National Cybercrime Action Plan 2016), Стратегией национальной кибербезопасности 2016 года (National Cybersecurity Strategy 2016), Актом о кибербезопасности 2018 года (Cybersecurity Act 2018). Экспертами отмечается политика «мягкого направления» интеграционных процессов в сфере кибербезопасности в АСЕАН со стороны Сингапура [14]: например, правительство инициировало размещение в Сингапуре штаб-квартиры Глобального комплекса инноваций Интерпола (INTERPOL Global Complex for Innovation, IGCI) – научно-исследовательского центра, занимающегося вопросами киберпреступности, инновационной подготовки, оперативной поддержки и партнерства, а также предложило в рамках сотрудничества АСЕАН с Интерполом выделять больше сотрудников правоохранительных органов государств-членов АСЕАН для службы в IGCI.

Кроме того, совместно с Японией и Великобританией Сингапур выступил учредителем и спонсором некоммерческой организации сотрудничества – The CyberGreen Institute [11]. Это учреждение собирает и предоставляет надежные статистические данные, измерения и оптимальные методы смягчения последствий кибератак заинтересованным операторам связи, национальным группам реагирования на кибератаки (Cyber Security Incident Response Teams, CSIRTs) и национальным и международным субъектам, определяющим политику в сфере кибербезопасности. В рамках проекта CyberGreen государства АСЕАН получают информацию о состоянии и потенциальных уязвимостях киберзащиты, что позволяет им предотвращать потенциальные киберриски. Со временем планируется разработка надежной методологии киберзащиты. Это позволит составить картину того, как каждое государство и АСЕАН в целом реагируют на киберугрозы, которые будут систематизироваться по классам опасности, поэтому национальным группам реагирования на кибератаки будет легче вырабатывать стратегию и тактику противодействия с учетом информации, предоставленной специалистами CyberGreen.

Будучи спонсором этой инициативы, Сингапур предоставляет государствам-участникам АСЕАН бесплатный доступ к данным проекта CyberGreen, а также первый отчет о состоянии национальной системы кибербезопасности. Это позволит государствам региона улучшить совместную работу по созданию безопасного киберпространства АСЕАН.

В своей Стратегии кибербезопасности от 2016 года Сингапур выделяет четыре основные опоры: (i) построение устойчивой инфраструктуры для усиления CII путем тесного сотрудничества частного сектора и представителей публичного сектора, уполномоченных на обеспечение кибербезопасности; (ii) создание безопасного киберпространства путем привлечения не только правительственных субъектов, но и гражданского общества и предпринимателей; (iii) развитие динамичной экосистемы кибербезопасности за счет увеличения количества специалистов в

результате сотрудничества частного сектора и образовательных заведений; (iv) усиление международного сотрудничества, особенно в рамках АСЕАН [24].

В список секторов CII Сингапур включил услуги (государственные и аварийные службы, здравоохранение, средства массовой информации, банковские и финансовые услуги), коммунальные услуги (энергетика, вода и телекоммуникации) и транспорт (наземный транспорт, морской и портовый, гражданская авиация) [24]. Акт о кибербезопасности 2018 года определяет секторы CII в рамках термина «существенные службы» (essential services), который означает любые службы, необходимые для национальной безопасности, обороны, внешних отношений, экономики, общественного здравоохранения, общественной безопасности или общественного порядка. Все эти службы перечислены в Перечне 1 к CSA (всего 46 в списке): они имеют отношение к энергетике, инфокоммуникациям, водоснабжению, здравоохранению, банковскому и финансовому обеспечению, безопасности и экстренной помощи, авиации, наземному транспорту, морскому транспорту, средствам массовой информации и услугам, связанным с функционированием правительства [12]. Принятию CSA предшествовали публичные обсуждения законопроекта с участием представителей частного сектора и общественности [23]. Их замечания были учтены, и в результате проект был серьезно доработан и принят в действующей редакции.

Существенным плюсом CSA является четкое терминологическое определение CII как «компьютера или компьютерной системы, которые полностью или частично находятся в Сингапуре, необходимы для непрерывного функционирования существенных служб, а их утеря контроля над ними или причинение им вреда окажет негативное влияние на доступность существенной службы» (раздел 2, раздел 7 (1)). CSA устанавливает сбалансированный институциональный механизм обеспечения кибербезопасности CII, во главе которого действует наделенный широкими полномочиями Комиссар по кибербезопасности (Commissioner on Cybersecurity, далее – Комиссар), занимающий одновременно пост директора Агентства по кибербезопасности Сингапура. В частности, его полномочия включают в себя 1) идентификацию и присвоение статуса CII; 2) осуществление контроля собственников CII в отношении кибербезопасности (секция 5 (e)); 3) разработка кодексов практики и стандартов обеспечения кибербезопасности собственниками CII (секция 5 (f)); 4) лицензирование и установление стандартов в отношении поставщиков услуг по кибербезопасности (секция 5 j)); 5) установление стандартов в отношении продуктов или услуг по обеспечению кибербезопасности, а также установление граничного уровня кибербезопасности для компьютерного оборудования или программного обеспечения, включая схемы сертификации или аккредитации (секция 5 (k)).

Наиболее важными разделами CSA являются разделы 3, 4 и 5. В разделе 3 устанавливаются правила идентификации CII и контроля собственников CII. В разделе 4 предусмотрен порядок принятия мер по предотвращению, регулированию и реагированию на киберугрозы и киберинциденты. В разделе 5 закреплен механизм лицензирования поставщиков услуг по обеспечению кибербезопасности.

В отношении идентификации CII Комиссар может письменно уведомить владельца компьютера или компьютерной системы о необходимости отнесения компьютера или компьютерной системы к CII. Чтобы удостовериться, соответствует ли компьютер или компьютерная система требованиям к CII, Комиссар имеет право истребовать необходимую информацию от владельца такого компьютера или компьютерной системы. Но CSA предоставляет владельцу CII право не предоставлять такую информацию в случае, если она защищена законом, контрактом или правилами профессионального поведения (секция 8 (5)). Однако договорные обязательства по-прежнему не являются основанием для отказа в раскрытии информации в контексте (i) запроса информации, относящейся к известной CII, или (ii) расследования киберинцидентов (секция 19 (6)). В соответствии с CSA владелец CII не будет считаться нарушающим такое договорное обязательство, если разглашение было сделано с разумной осторожностью и добросовестностью. Однако эти положения по-прежнему вызывают беспокойство у владельцев CII насчет защиты их коммерческой информации. CSA требует от них сообщать о киберинцидентах, перечень которых издает Комиссар. Ранее законопроект CSA требовал предоставления информации обо всех «значительных» киберпроисшествиях [25].

Комиссар также уполномочен издавать письменные указания, которые могут касаться: (a) действий, предпринимаемых владельцем или владельцами CII в связи с угрозой кибербезопасности; (b) соблюдения владельцем или владельцами CII любого кодекса практики или стандарта; (c) назначения аудитора, утвержденного Комиссаром, для проверки владельца или владельцев CII на предмет соблюдения ими CSA или любого кодекса практики или стандарта; (d) любых других вопросов, которые он сочтет необходимыми или целесообразными для обеспечения кибербезопасности CII (секция 12).

В соответствии с CSA каждая CII должна подвергаться аудиту не реже одного раза в два года и оценке рисков один раз в год для подтверждения соответствия законодательству. Аудитор утверждается или назначается Комиссаром (секция 15). В случае отказа владельца CII от прохождения аудита предусмотрена уголовная ответственность в виде штрафа до 100 тыс. долл. США и/или лишения свободы на срок до 2 лет, а в случае продолжающегося преступления – дополнительно штраф, не превышающий 5 тыс. долл. США за каждый день (или часть дня), в течение которого правонарушение продолжается после предъявления обвинения.

Профилактика киберинцидентов осуществляется путем проведения обязательных учений с целью проверки состояния готовности владельцев CII. В случае уклонения от таких учений владелец CII несет ответственность в виде штрафа до 100 тыс. долл. США (секция 16). В случае киберугроз или киберинцидентов (в том числе, серьезных) Комиссар уполномочен их расследовать путем: (1) получения подписанных заявлений, физических или электронных записей и документов; (2) опроса лиц, которые могут иметь информацию о фактах и обстоятельствах киберугроз (киберинцидентов); (3) назначения технических экспертов по кибербезопасности; (4) привлечения необходимых специалистов из всех правоохранительных и силовых подразделений Сингапура и проч. (секции 19, 20, 22). Секция 23

устанавливает особенности реализации полномочий правоохранительных органов в случае противодействия киберугрозам, а также предусматривает ответственность лиц, не выполняющих законные требования правоприменителей (штраф до 50 тыс. долл. США и/или лишение свободы до 10 лет).

Еще одной особенностью CSA, которая определяет его стандартом нового поколения, является обязательное лицензирование поставщиков услуг по кибербезопасности (секция 24). Лицензированию подлежат (a) службы мониторинга управляемых центров безопасности (managed security operations centre (SOC) monitoring service) и (б) служба тестирования на взлом (penetration testing service). CSA предусматривает три типа лицензий: (a) общая (условия применимы ко всем лицензиатам); (b) специальная (условия применимы к определенному классу лицензиатов) и (c) индивидуальная (условия применимы только к указанному лицензиату). Лицензия действует в течение определенного периода, но не более 5 лет. Лицензиат обязан выполнять требования, предъявляемые CSA (прежде всего, обязанность вести учет информации, необходимой для защиты CII, в течение трех лет), и в противном случае может быть подвергнут штрафу до 10 тыс. долл. США и/или лишению свободы на срок до 12 месяцев.

Программа АСЕАН по увеличению киберпотенциала стоимостью более 7 млн долл. США, инициированная Сингапуром в 2017 году, рассчитана на 5 лет. Она направлена на увеличение киберпотенциала каждого государства-участника АСЕАН и будет содействовать увеличению способностей региона в целом противодействовать киберугрозам.

Программа предусматривает серию мероприятий и инициатив по развитию технического, политического и стратегического потенциалов государств-участников АСЕАН по следующим направлениям: политика в сфере кибербезопасности, законодательство, развитие стратегии и реакций на киберугрозы. Семинары и конференции рассчитаны на политиков, дипломатов, прокуроров, технических операторов и аналитиков. Тренеры представлены лучшими специалистами из Глобального центра инноваций Интерпола (INTERPOL Global Centre for Innovation in Singapore), Агентства кибербезопасности Сингапура (the Cyber Security Agency of Singapore), Центра передового опыта в области национальной безопасности Школы международных отношений им. С. Раджаратнама (Centre of Excellence for National Security (CENS) at the S.Rajaratnam School of International Studies (RSIS)) и других учреждений.

Важным мероприятием данной программы является Сингапурская международная кибернеделя (Singapore International Cyber Week), во время которой проходят Министерская конференция АСЕАН по кибербезопасности и Воркшоп по кибербезопасности (Cybersecurity Workshop) – совместный проект Сингапура и США [16].

Выводы

Вышесказанное позволяет сделать следующие выводы. Во-первых, национальный механизм кибербезопасности Сингапура имеет самую длительную по сравнению с другими государствами-участниками АСЕАН историю становления. Это обусловлено темпами социально-экономического развития государства, его

фактическим статусом регионального и международного торгово-экономического центра. Сингапур реализует модель публично-частного партнерства обеспечения кибербезопасности, где государству отведена роль политико-направляющего субъекта (например, при определении секторов CII), мнение представителей частного сектора играет решающую роль при определении содержания нормативного механизма кибербезопасности, а сами они включены в институционный механизм обеспечения кибербезопасности. Во-вторых, законодатель смог найти баланс в обеспечении публичных интересов и защите гражданских прав и свобод, что очень важно в условиях сохранения и увеличения инвестиционной привлекательности государства. И, наконец, определение регионального и международного сотрудничества в качестве одной из четырех опор стратегии кибербезопасности и запуск ряда успешных проектов в этой сфере делают Сингапур лидером не только в АСЕАН, но и на международной арене. На наш взгляд, сохранение текущего status quo, а в перспективе – дальнейшее развитие этого направления внешней политики Сингапура способны вывести это государство на ведущие позиции при разработке универсального международно-правового механизма обеспечения кибербезопасности.

1. Гуревич Э.М. Основные аспекты внешней политики Сингапура в 2007–2008 гг. // Юго-Восточная Азия: актуальные проблемы развития. 2009. № 12. С. 186–208.
2. Костюнина Г.М. Государственная поддержка инвестиционных проектов в странах АСЕАН // Юго-Восточная Азия: актуальные проблемы развития. 2017. № 36. С. 24–34.
3. Костюнина Г.М. Экономическое сообщество АСЕАН: направления и перспективы формирования // Российский внешнеэкономический вестник. 2015. Т. 2015. № 12. С. 14–31.
4. Курский С.Н. Зоны свободной торговли АТЭС и АСЕАН и перспективы участия в них Российской Федерации // Финансы и кредит. 2006. № 24 (228). С. 43–48.
5. Савельев А.А. Экономическая интеграция в Юго-Восточной Азии и ее значение для расширения внутрирегионального инвестиционного сотрудничества // Наука и бизнес: пути развития. 2015. № 4 (46). С. 121–126.
6. Фатуллаев Д.Г. Внешнеторговое сотрудничество между Россией и странами АСЕАН: основные тенденции развития // Экономика и предпринимательство. 2018. № 4 (93). С. 94–98.
7. Bobro D. Methodological aspects of critical infrastructure protection // Research Gate [Электронный ресурс]. URL: https://www.researchgate.net/publication/322715607_The_National_Institute_for_Strategic_Studies_methodological_aspects_of_critical_infrastructure_protection.
8. Catastrophic cascade of failures in interdependent networks / S.V. Buldyrev, R. Parshani, G. Paul, H.E. Stanley, S. Havlin // Nature. 2010. №464 (7291). Pp. 1025–1028
9. Chairman's Statement of the 32nd ASEAN Summit (Singapore, 28 April 2018) // ASEAN Singapore 2018 [Электронный ресурс]. URL: https://www.asean2018.sg/Newsroom/Press-Releases/Press-Release-Details/20180428_Chairmans_Statement.
10. Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European Critical Infrastructures and the assessment of the need to improve their protection. Official Journal L, 345(23), 12.

11. Cybergreen // The CyberGreen Institute [Электронный ресурс]. URL: https://www.cybergreen.net/
12. Cybersecurity Act 2018 // Cyber Security Agency of Singapore [Электронный ресурс]. URL: https://www.csa.gov.sg/legislation/cybersecurity-act
13. Cybersecurity 2018 : Indonesia // International Comparative Legal Guides[Электронный ресурс]. URL: https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/indonesia
14. Cybersecurity in ASEAN: An Urgent Call to Action / N. Dobberstein, D. Gerdemann, G. Pereira, G. Hoe // ATKearney [Электронный ресурс]. URL: http://www.southeast-asia.atkearney.com/paper/-/asset_publisher/dVxv4Hz2h8bS/content/cybersecurity-in-asean-an-urgent-call-to-action
15. e-Conomy SEA Spotlight 2017: Unprecedented growth for Southeast Asia's $50B internet economy [report by Google and TEMASEK] // ASEAN UP [Электронный ресурс]. URL: https://aseanup.com/southeast-asia-digital-economy-2017/
16. Factsheet on ASEAN Cyber Capacity Programme // Cyber Security Agency of Singapore [Электронный ресурс]. URL: https://www.csa.gov.sg/~/media/csa/documents/amcc/factsheet_accp.ashx
17. Farrand B., Carrapico H. Blurring Public and Private: Cybersecurity in the Age of Regulatory Capitalism // Security Privatization: How Non-Security-Related Private Businesses Shape Security Governance. Basel: Springer International Publishing AG, 2018. Pp. 197–217.
18. Green Paper on a European Programme for Critical Infrastructure Protection. COM 576 final (2005).
19. Iwamoto K. Rise of digital economy pushes ASEAN toward policy coordination // NIKKEI: Asian Review [Электронный ресурс]. URL: https://asia.nikkei.com/Politics/Rise-of-digital-economy-pushes-ASEAN-toward-policy-coordination2
20. Matania E., Yoffe L., Goldstein T. Structuring the national cyber defence: in evolution towards a Central Cyber Authority // Journal of Cyber Policy. 2017. № 2(1). Pp. 16–25.
21. Mattioli R., Levy-Bencheton C. Methodologies for the identification of Critical Information Infrastructure assets and services: Guidelines for charting electronic data communication networks. – Heraklion: European Union Agency for Network and Information Security (ENISA), 2014. 43 p.
22. Nguyen M. Vietnam lawmakers approve cyber law clamping down on tech firms, dissent // REUTERS [Электронный ресурс]. URL: https://www.reuters.com/article/us-vietnam-socialmedia/vietnam-lawmakers-approve-cyber-law-clamping-down-on-tech-firms-dissent-idUSKBN1J80AE
23. Report on Public Consultation on the Draft Cybersecurity Bill, issued by the Ministry of Communications and Information and the Cyber Security Agency of Singapore, 13 November 2017 // Government of Singapore [Электронный ресурс]. URL: https://www.reach.gov.sg/participate/public-consultation/ministry-of-communications-and-information/public-communications-division/public-consultation-paper-on-the-draft-cybersecurity-bill
24. Singapore's Cybersecurity Strategy 2016 // Cyber Security Agency of Singapore [Электронный ресурс]. URL: https://www.csa.gov.sg/news/publications/singapore-cybersecurity-strategy
25. Singapore's New Cybersecurity Act – A Relief and Leading the Way for Others? // BakerMcKenzie [Электронный ресурс]. URL: https://www.bakermckenzie.com/en/insight/publications/2018/02/singapores-new-cybersecurity-act

26. Toomgum S. Thailand among top 20 nations focusing on cybersecurity // The Nation [Электронный ресурс]. URL: http://www.nationmultimedia.com/detail/Economy/30325029

Транслитерация

1. Gurevich E.M. Osnovnye aspekty vneshnei politiki Singapura v 2007-2008 gg., *Yugo-Vostochnaya Aziya: aktual'nye problemy razvitiya*, 2009, No 12, pp. 186–208.
2. Kostyunina G.M. Gosudarstvennaya podderzhka investitsionnykh proektov v stranakh ASEAN, *Yugo-Vostochnaya Aziya: aktual'nye problemy razvitiya*, 2017, No 36, pp. 24–34.
3. Kostyunina G.M. Ekonomicheskoe soobshchestvo ASEAN: napravleniya i perspektivy formirovaniya, *Rossiiskii vneshneekonomicheskii vestnik*, 2015, vol. 2015, No 12, pp. 14–31.
4. Kurskii S.N. Zony svobodnoi torgovli ATES i ASEAN i perspektivy uchastiya v nikh Rossiiskoi Federatsii, *Finansy i kredit*, 2006, No 24 (228), pp. 43–48
5. Savel'ev A.A. Ekonomicheskaya integratsiya v Yugo-Vostochnoi Azii i ee znachenie dlya rasshireniya vnutriregional'nogo investitsionnogo sotrudnichestva, *Nauka i biznes: puti razvitiya*, 2015, No 4 (46), pp. 121–126.
6. Fatullaev D.G. Vneshnetorgovoe sotrudnichestvo mezhdu Rossiei i stranami ASEAN: osnovnye tendentsii razvitiya, *Ekonomika i predprinimatel'stvo*, 2018, No 4 (93), pp. 94–98.

Для цитирования: Горян Э.В. Ведущая роль Сингапура в обеспечении кибербезопасности в АСЕАН: промежуточные результаты и перспективы дальнейшего расширения // Территория новых возможностей. Вестник Владивостокского государственного университета экономики и сервиса. 2018. Т. 10. № 3. С. 103–117.

For citation: Gorian E.V. Singapore's leadership on cybersecurity in ASEAN: intermediate results and future prospects, *The Territory of New Opportunities. The Herald of Vladivostok State University of Economics and Service*, 2018, Vol. 10, No 3, pp. 103–117.

DOI dx.doi.org/10.24866/VVSU/2073-3984/2018-3/103-117

Дата поступления: 30.07.2018.