СИБ СКРИПТ

2024 ТОМ 26 № 3

оригинальная статья

https://elibrary.ru/rpegey

Эволюция инфраструктуры информационной и кибербезопасности Индии

Матюхина Елена Николаевна

Тюменский государственный университет, Россия, Тюмень

eLibrary Author SPIN: 6020-8177

https://orcid.org/0000-0001-7565-0030

ematyuhina@mail.ru

Аннотация: Геополитические особенности положения Российской Федерации диктуют приоритетные направления потенциального взаимовыгодного сотрудничества, Азиатско-Тихоокеанское – одно из них. Все более значимым игроком на мировой информационной арене является Индия, с которой России предстоит выстраивать обновленные и гарантированно безопасные линии сотрудничества. Данная работа является частью задуманной серии публикаций и выполнена с целью исследования системы информационной безопасности Индии и ее особенностей. Цель – определить контуры, очертания системы информационной безопасности, созданной государством и соответствующими структурами Индии за последние десятилетия. В ходе исследования описаны этапы формирования концепции информационной безопасности Индии, выявлены механизмы, обеспечивающие информационную безопасность страны, исследованы механизмы, обеспечивающие экономическую безопасность страны, описаны инструменты, обеспечивающие безопасность Индии в сфере защиты баз данных в глобальном информационном пространстве. Данное исследование предоставляет полную картину поэтапного выстраивания структуры информационной безопасности Индии в различных сферах и отраслях. По последовательности их учреждения и вступления в силу были затронуты все основные действующие и разрабатываемые механизмы обеспечения защиты каждого сектора киберпространства страны. Детально описаны их функции и цели: различного рода нормативно-правовые акты (от свода правил до национальных доктрин) или органы по регулированию описываемой сферы информационной безопасности. Представлен целостный взгляд на развитие концепции информационной безопасности страны по ее внешним пределам с концентрацией на хронологическом повествовании о каждой стадии ее формирования. Информация изложена с конкретным разделением всех основных ныне присутствующих в стране механизмов на отдельные группы.

Ключевые слова: информационная безопасность, кибербезопасность, концепция, этапы, механизмы, инструменты, глобальные угрозы

Цитирование: Матюхина Е. Н. Эволюция инфраструктуры информационной и кибербезопасности Индии. *СибСкрипт*. 2024. Т. 26. № 3. С. 441–458. https://doi.org/10.21603/sibscript-2024-26-3-441-458

Поступила в редакцию 29.12.2023. Принята после рецензирования 01.03.2024. Принята в печать 11.03.2024.

full article

Evolution of India’s External Information and Cyber Security Infrastructure

Elena N. Matyukhina

Tyumen State University, Russia, Tyumen

eLibrary Author SPIN: 6020-8177

https://orcid.org/0000-0001-7565-0030

ematyuhina@mail.ru

Abstract: The geopolitical situation of the Russian Federation dictates the priority areas of potential mutually beneficial cooperation, the Asia-Pacific being one of them. India’s role on the global information arena is increasing, and Russia needs to set up new, secure lines of cooperation. This work is part of a series of publications on India’s information

security system. The article outlines its progress over the past decades, e.g., the concept of information security, the mechanisms that ensure India's external information and economic security, the tools of database protection in the global information environment, etc. The result is a complete and comprehensive picture of the stage-by-stage development of India's information security structure in various fields and industries in each sector of cyberspace, with goals and functions for each regulatory act and control institution. This holistic view of India's information security covers its concept and chronology of development, as well as offers a classification of the key information security mechanisms currently active in the country.

Keywords: information security, cyber security, concept, stages, mechanisms, tools, global threats

Citation: Matyukhina E. N. Evolution of India's External Information and Cyber Security Infrastructure. *SibScript*, 2024, 26(3): 441–458. (In Russ.) https://doi.org/10.21603/sibscript-2024-26-3-441-458

Received 29 Dec 2023. Accepted after peer review 1 Mar 2024. Accepted for publication 11 Mar 2024.

Введение

В век информационных технологий состояние защищенности и сохранности информации становится одним из основных приоритетов государств по всему миру. Развитие информационной и кибербезопасности все сильнее набирает ход в ответ на столь же быстрорастущее число киберпреступлений. В связи со сложившейся нестабильной обстановкой перспективным становится путь межгосударственного взаимодействия в области развития ИТ-технологий и обустройства системы информационной безопасности государства. Учитывая геополитические особенности положения, в котором находится Российская Федерация, приоритетным направлением потенциального взаимовыгодного сотрудничества становится Азия. Все более значимым игроком на мировой информационной арене является Индия, с которой России предстоит выстраивать обновленные линии сотрудничества.

Страна за последние десятилетия приобрела статус одного из лидеров ИТ-индустрии. Чтобы заметить рост в позиции Индии, достаточно отметить то, что Индийский среднегодовой темп увеличения числа предприятий ИТ-сегмента составляет 8–9 %. Государство называют новым информационным чудом, их онлайн-рынок является вторым в мире. Уступая лишь Китаю, он насчитывает свыше 560 млн интернет-пользователей. Однако многочисленные внешние угрозы и полноценные атаки, доходя до рекордных показателей в мире, красноречиво подчеркивают малую заинтересованность Индии в вопросах информационной безопасности. Ситуация постепенно начала меняться на стыке первых десятилетий XXI в. с приходом в Индию новых инициатив по развитию системы кибербезопасности.

Цель – определить контуры, очертания системы информационной безопасности, созданной государством и соответствующими структурами Индии за последние десятилетия. Для ее достижения были поставлены и выполнены следующие задачи: описаны этапы формирования концепции информационной безопасности Индии; выявлены механизмы, обеспечивающие информационную безопасность страны; обозначены инструменты обеспечения информационной безопасности Индии от внешних угроз. В частности, последний пункт разделен на две подтемы: выявление механизмов, обеспечивающих экономическую безопасность страны, а также механизмов, обеспечивающих безопасность Индии в сфере защиты баз данных в глобальном информационном пространстве.

В работе [Shukla, Agrawal 2020] собраны сведения не только о предпосылках и зарождении полноценной системы обеспечения информационной безопасности в Индии, но и о новейших инструментах и угрозах кибербезопасности страны и ее граждан. Отечественные авторы также внесли вклад в изучение информационной безопасности Индии[1] [Бухарин 2019; Дементьев, Яркин 2017; Замулина 2023; Зиновьева, Игнатов 2023; Казарин, Тарасов 2013; Маланичева и др. 2023; Михайлова, Горбунова 2019; Никипорец-Такигава и др. 2023; Перминов 2019; Ревенко, Ревенко 2017;

[1] Ярмолинский Ю. А. О некоторых аспектах обеспечения информационной безопасности в Индии. *Белорусский институт стратегических исследований*. 27.11.2019. URL: https://bisr.gov.by/mneniya/o-nekotorykh-aspektakh-obespecheniya-informacionnoy-bezopasnosti-v-indii; Муратбекова А. Обсуждение тенденций развития кибербезопасности Индии. *Eurasian Research Institute*. 13.03.2022. URL: https://www.eurasian-research.org/publication/discussion-of-indias-cyber-security-development-trends/?lang=ru (дата обращения: 15.11.2023).

Сахаров 2023; Суюнова 2022]. Значительная доля в исследовании обозначенной темы принадлежит зарубежным авторам [Bhattacharjee 2023; Godse 2010; ICT with Intelligent Applications 2022; Kumar, Inbaraj 2018; Lessambo 2023; Mishra et al. 2016; Patil 2021; 2022; Shukla, Agrawal 2020]. Организации, обратившие в своих статьях внимание на рассматриваемый вопрос: Евразийский исследовательский институт, научно-технический центр ФГУП «ГРЧЦ», Белорусский институт стратегических исследований, Уральский центр систем безопасности[2].

Все проанализированные источники можно объединить в несколько групп. Так, основным источником предоставленной информации выступают многочисленные ресурсы, находящиеся в открытом доступе в сети Интернет. В рамках этой группы были проанализированы различные подтипы статей: информационные, аналитические, образовательные, юридические, форумные. Среди используемых интернет-ресурсов стоит отметить Российский совет по международным делам[3], Уральский центр систем безопасности, Евразийский юридический журнал и др.

Следующая группа источников предоставляет статистические выкладки в области информационной безопасности. Для этого использовались материалы международного форума Global Cybersecurity Index, освещающего позиции государств в международном информационном пространстве.

Третья группа предоставлена научными работами [Казарин, Тарасов 2013; Перминов 2019].

Для анализа зарубежных трудов главным ресурсом выступает издательство Springer. В исследовании использовались как отдельные научные статьи, так и целые сборники лекций и статей на тему информационной безопасности. Основная часть информации для анализа представлена в книге «Кибербезопасность в Индии» ведущих специалистов области – Сандип Кумар Шукла и Маниндра Агравал [Shukla, Agrawal 2020]. Однако не менее важную роль имеют работы [Суюнова 2022; Kumar, Inbaraj 2018; Mishra et al. 2016; Patil 2022; Prasad, Kumar 2022; Reghunadhan 2022].

Для изучения непосредственного государственного регулирования в аспектах информационной безопасности в Индии были изучены официальные сайты государства, такие как Министерство электроники и информационных технологий от государственного управления Индии[4]. В частности, использовались сайты отделов кибербезопасности и киберзаконов, а также сторонние сайты, предоставляющие доступ к копиям документов[5] (например, консорциум «Кодекс»). Анализ и информационное сопровождение для исследуемых документов предоставлены на образовательном ресурсе wiki5.ru и статье «Республика Индия» научно-технического центра ФГУП «ГРЧЦ»[6].

В рамках данной группы стоить отметить Меморандум о взаимопонимании между Индией и США в 2011 г., Национальную политику Индии в области кибербезопасности 2013 г., Соглашение между Правительством Российской Федерации и Правительством Республики Индии о сотрудничестве в области обеспечения безопасности в сфере использования информационно-коммуникационных технологий от 2016 г. (вступившее в силу в 2017 г.), которое является серьезной вехой для индийско-российских отношений. В числе основных направлений сотрудничества указаны: определение, координация и осуществление необходимых мер по обеспечению безопасности в сфере использования информационно-коммуникационных технологий (ИКТ); создание системы защищенного обмена информацией, которой располагают Стороны о подобных нападениях, об их источниках, исполнителях и о снижении последствий инцидентов и нападений с использованием ИКТ; содействие выработке мер в области ограничения распространения и использования вредоносных средств и уязвимостей в сфере использования ИКТ, которые могут угрожать национальной и общественной безопасности, в том числе на международном уровне; противодействие угрозам использования ИКТ в террористических целях и др.

Последней, но немаловажной группой являются публикации новостных изданий, освещающих важные события в области информационной безопасности

[2] Баклушин Е. А. Критическая информационная инфраструктура Индии. *Уральский центр систем безопасности*. 11.05.2022. URL: https://www.ussc.ru/news/novosti/kriticheskaya-informatsionnaya-infrastruktura-indii/ (дата обращения: 15.11.2023).

[3] Карасев П. Кибербои без правил. *Российский совет по международным делам*. 24.07.2019. URL: https://russiancouncil.ru/analytics-and-comments/analytics/kiberboi-bez-pravil/ (дата обращения: 15.11.2023).

[4] Ministry of Electronic & Information Technology. URL: https://www.meity.gov.in/ (accessed 15 Nov 2023).

[5] Information Technology Act, 2000. URL: https://www.itlaw.in/ (accessed 15 Nov 2023).

[6] Республика Индия. *Научно-технический центр ФГУП «ГРЧЦ»*. 14.10.2020. URL: https://rdc.grfc.ru/2020/10/india/#post-758-_Toc49359825 (дата обращения: 15.11.2023).

Индии[7]. Особую значимость для исследования имеют публикации и статьи Тасс.ру, РИА новости, информационного агентства «Красная весна», Регнум.ру[8], при помощи данных ресурсов удалось собрать для анализа немалое количество сведений для разбора, статистики и знаменательных событий в стране.

Многие аспекты системы информационной безопасности Индии открыты для ознакомления. Устройство органов по обеспечению и надзору за информационной безопасностью государства, их правовое регулирование, стратегию страны в рассматриваемом вопросе, как и многое другое, возможно найти в сети Интернет [Авешникова 2018].

Для выполнения перечисленных задач были использованы: сбор, обработка и анализ многочисленных материалов по теме; систематизация и анализ источников и литературы. В работе использовались как общенаучные, так и специальные методы исследования: анализ, синтез, сравнение, обобщение и систематизация, а также такие эмпирические методы, как анализ нормативных документов, метод анализа событийных данных – ивент-анализ.

Результаты

В ходе исследования было поэтапно описано формирование концепции информационной безопасности Индии. В качестве отдельных этапов были взяты ключевые события, относящиеся к системе информационной безопасности страны. Среди стадий представлены: формирование и принятие нормативно-правовых актов отрасли; учреждение новых государственных и независимых органов, агентств и организаций, ведущих деятельность непосредственно в среде информационной безопасности или касающихся ее; принятие национальных доктрин (стратегий и национальных политик развития сектора); ключевые события в международном взаимодействии – заключение соглашений, пактов, меморандумов и т. д. Каждый этап описан последовательно, начиная с принятия первого важнейшего закона в области информационно-коммуникационных технологий в 2000 г. и заканчивая событиями 2022–2023 гг.

В данном исследовании мы ориентировались на хронологические рамки 2008–2022 гг. Нижняя хронологическая рамка определяется датой обширных поправок в основном законодательном акте Индии, регулирующем правоотношения в сфере информационных технологий – Законе об информационных технологиях (Information Technology Act). Вступивший в силу в 2002 г., данный нормативно-правовой акт более двух десятилетий является основным столпом регулирования кибербезопасности государства. В 2008 г. он получил существенные поправки, что предзнаменовало более глобальные изменения в отрасли[9].

Однако основной отправной точкой исследования можно считать 2012 г., когда Индия решила перейти на более самостоятельное обеспечение информационной безопасности страны. На Мюнхенской конференции этого года индийские специалисты официально заявили о ведущихся работах по сокращению импорта в сфере кибербезопасности и намерении обеспечить значимое спонсирование собственных разработок. Этот год ознаменован созданием центра командования и контроля для мониторинга критической инфраструктуры и ликвидации брешей в киберзащите государства. С этого момента Индия берет курс на усиленное развитие исследуемого направления.

Верхняя рамка исследования обуславливается изучением состояния системы кибербезопасности Индии на данный момент (2022 г.).

Полученные нами результаты во многом соотносятся и обобщают опыт изучения темы отечественными и зарубежными коллегами, который подробно анализировался при подготовке материала. Интернет в Индии появился в 1986 г. Экономические реформы, начатые в 1991 г., оказали свое влияние, и в Индии был дан старт развитию индустрии программного обеспечения, стали появляться первые в стране ИТ-компании. Это способствовало росту использования Интернета в Индии[10].

Уже на ранних этапах многие государства, в первую очередь западные, пытались регулировать эту сеть. Их усилия были объединены в Международном союзе электросвязи (МСЭ), который возник как первая

[7] Индия пересматривает нацполитику кибербезопасности. *Новости Узбекистана*. 16.09.2020. URL: https://nuz.uz/2020/09/16/indiya-peresmatrivaet-naczpolitiku-kiberbezopasnosti/ (дата обращения: 15.11.2023).

[8] Исаев М. М. Economist: Индия столкнулась с опасными вызовами в сфере кибербезопасности. *Регнум.ру*. 02.11.2019. URL: https://regnum.ru/news/2766808.html (дата обращения: 15.11.2023).

[9] Федотов А. А. Опыт регулирования информационного пространства в Индии. *D-russia.ru*. 14.10.2020. URL: https://d-russia.ru/opyt-regulirovanija-informacionnogo-prostranstva-v-indii.html (дата обращения: 15.11.2023).

[10] Борисова М. В. Миллионы IT-шников, отключения, дешевая связь, – как устроен интернет в Индии. *Сайт TexTerra.ru*. 03.06.2022. URL: https://texterra.ru/blog/internet-v-indii-99-pokrytiya-borba-s-kitaem-tsenzura.html (дата обращения: 12.01.2023).

https://doi.org/10.21603/sibscript-2024-26-3-441-458

международная организация, обсудившая последствия зарождения нового этапа технологической эволюции (ITU, 1999).

Несмотря на быстрое расширение использования Интернета, индийские политические деятели только начинали постигать новую веху технологий, о чем свидетельствует низкий уровень участия страны в многосторонних форумах, таких как МСЭ и Всемирный саммит по информационному обществу, который являлся форумом для правительственных консультаций по вопросам ИТ, кибер- и цифровых технологий.

В то же время пользователи Интернета делают первые шаги в сторону преступлений в цифровом пространстве[11]. Стремительное развитие Интернета и связанные с ним преступления нуждались в регулировании, поэтому для решения проблем преступности в киберпространстве возникла новая отрасль юриспруденции – киберправо, или право информационных технологий.

На тот момент министр парламентских дел и министр информационных технологий Шри Прамод Махаджан во время обсуждения законопроекта об информационных технологиях в 1999 г. говорил об отсутствии в Индии подходящего закона для борьбы с фальсификацией компьютерных исходных документов, публикацией информации непристойного характера и по вопросам, связанным с повреждением компьютеров и компьютерных сетей, с помощью системы соответствующих штрафов и наказаний. В развитие этой идеи и для приведения законодательства в соответствие с Типовым законом об электронной коммерции, принятым комиссией ООН по праву международной торговли, в Индии был принят Закон об информационных технологиях 2000 г.[12] (Information Technology Act, 2000).

Закон об ИТ был принят парламентом 15 мая 2000 г., утвержден президентом Кочерилом Раманом Нараянаном 9 июня 2000 г. и введен в действие 17 октября того же года[13]. С его введением в действие были внесены поправки в следующие четыре закона индийского законодательства, доставшиеся современной Индии в наследство из ее колониального прошлого: Уголовный кодекс Индии (1860); Закон Индии о доказательствах (1872); Закон о доказательствах в банковских книгах (1891); Закон о Резервном банке Индии (1934). Текст законов был составлен по нормам британского права, поэтому до наступления эры информационных технологий устраивал всех, кто пользовался ими в своей деятельности. Систематизация колониального права Индии была комплексной и межотраслевой, она содержала элементы как кодификации, так и консолидации. Успешность УК Индии на практике была связана с систематическим подходом реформаторов, которые параллельно выработали такие базовые акты, как Гражданско-процессуальный кодекс (1859), Уголовно-процессуальный кодекс (1861), консолидированные Законы о полиции (1861) и доказательствах (1872) и др. В основе успеха этой широкомасштабной межотраслевой систематизации и унификации права лежали веские утилитарные причины, прежде всего необходимость обеспечить надежное управление и правопорядок на обширной территории нестабильных индийских княжеств. С введением законодательства об ИТ в силу Индия становится двенадцатой страной мира, принявшей реалии киберправа.

Закон об ИТ предоставляет правовую базу для электронной коммерции и обеспечения безопасного использования электронных документов и любой формы электронной коммуникации. Закон охватывает такие вопросы, как незаконный доступ к компьютерной информации, электронное мошенничество, киберпреступления, нарушения авторских прав, кражу личной информации, соответствующие меры наказания. Закон предоставляет защиту персональных данных и конфиденциальности, определяет обязательства компаний по защите данных клиентов и устанавливает процедуры обязательного уведомления о нарушениях безопасности данных.

Создание структур, обеспечивающих информационную безопасность Индии

Начало XXI в. принесло осознание, что пространство информационных технологий становится новым полем для разногласий, конфликтов и преступности. Киберугроза к тому времени уже существовала. В Индии совершались преступления в киберпространстве. Некоторые из наиболее серьезных инцидентов включали в себя хакерскую атаку на сайт Индийского

[11] Куприянов А. Б. Индия в эпоху кибервойн. *Российский совет по международным делам*. 07.08.2019. URL: https://russiancouncil.ru/analytics-and-comments/analytics/indiya-v-epokhu-kibervoyn/ (дата обращения: 15.11.2023).

[12] Information Technology (Intermediary Guidelines) Rules, 2011. URL: https://www.itlaw.in/https-www-itlaw-in-information-technology-intermediaries-guidelines-rules-2011/ (accessed 15 Nov 2023).

[13] Global Cybersecurity Index 2020. URL: https://nonews.co/wp-content/uploads/2021/09/GCI2020.pdf (accessed 16 Nov 2023).

института технологий в Дели в 2001 г., взломы крупных компаний Satyam Computers и BSNL, потерявших такие данные, как финансовые отчеты и персональная информация клиентов. Кроме того, Индия числилась в ряду стран, наиболее пострадавших от крупнейших вирусов того времени: I Love You (2000) и Nimda (2001). Ситуация продолжала ухудшаться, и к 2004 г. Индия стала одной из наиболее уязвимых стран в мире по вопросам информационной безопасности.

В связи с плачевной ситуацией Индия начинает следующий этап развития своей инфраструктуры кибербезопасности. Он обозначается формированием государственных структур, которые будут вести свою деятельность в соответствии с созданной основой законодательства в области информационной безопасности. Первым таким органом становится новое подразделение министерства электроники и информационных технологий правительства Индии (MeitY) – группы реагирования на компьютерные чрезвычайные ситуации (CERT-IN, или ICERT). Она была организована как центральное агентство по борьбе с угрозами кибербезопасности, состав и руководство группы назначаются непосредственно правительством Индии. Акт об ИТ описывает ее функции как организации, призванной обеспечить безопасность киберпространства. CERT-IN также предоставляет консультации и рекомендации по улучшению информационной безопасности для государственных органов, частных компаний и общественности в целом, а предоставление ими услуг осуществляется в круглосуточном режиме.

Октябрь 2006 г. ознаменовался формированием учрежденного законом об ИТ Апелляционного суда по киберрегулированию (CRAT). В октябре 2006 г. этот орган был создан для рассмотрения спорных ситуаций, связанных с преступностью в информационной среде. Основная задача суда – предоставление платформы для разрешения инцидентов с цифровыми подписями и электронными транзакциями, его решения окончательны и обязательны к исполнению.

Первые учреждения были созданы для того, чтобы увеличить уровень защиты государственной информации и предотвратить кибератаки на важные объекты Индии. Однако не меньше внимания они уделяли и защите личных данных интернет-пользователей. Начальный этап создания системы информационной безопасности страны сформировал ее опору, фундамент для развития.

Тем не менее роль Индии в области защищенности информационной сферы была отстающей, и не стихающий глобальный рост киберпреступности особенно ярко демонстрировался на примере Индии. Каждая третья индийская организация несла финансовые убытки из-за кибератак, а зарубежные заказчики все чаще сталкивались с утечкой того или иного рода информации в результате взаимодействия с индийскими специалистами, что приводило к финансовым неудачам.

Законодательные меры по защите информации

В начале 2000-х гг. Индия сталкивается и с обострением угрозы кибертерроризма. В частности, был зарегистрирован первый случай кибератаки на индийскую военную систему; в 2008 г. произошли блокировки официальных сайтов правительства и крупных государственных компаний.

В связи с этим Индия начинает новый этап совершенствования системы информационной безопасности. Первой вехой в 2008 г. становятся крупные поправки в Закон об информационных технологиях от 2000 г. Среди основных положений было введение более жестких наказаний за киберпреступления, такие как мошенничество, кража личных данных, кибертерроризм и другие формы нарушений в интернет-пространстве. Были введены более высокие штрафы и увеличены сроки тюремного заключения в целях усиления борьбы с киберпреступностью. Немаловажным пунктом стал фокус на защиту данных – были внедрены новые механизмы предотвращения кражи данных – регуляция хранения и защиты личной информации и *чувствительных* данных от мошенничества. Поправки 2008 г. сделали Интернет в стране более защищенным и безопасным для пользователей.

Законодательство Индии пополнилось и в 2011 г. принятием нового документа – Правил информационных технологий (Information Technology Rules)[14]. Специфика данного нормативно-правового акта состояла в следующих пунктах:

1. Обеспечение конфиденциальности данных: правила 2011 г. содержат обновленные требования относительно условий обеспечения организациями достаточной меры конфиденциальности информации, которую они собирают и обрабатывают.

2. Развитие кибербезопасности: закон содержит положения о требованиях для организаций

[14] Elmokadem L., Naidu S. Mapping of India's cyber security-related bilateral agreements. *The Centre for Internet & Society*. 29 Dec 2016. URL: https://cis-india.org/internet-governance/blog/india-cyber-security-bilateral-agreements-map-dec-2016 (accessed 16 Nov 2023).

https://doi.org/10.21603/sibscript-2024-26-3-441-458

и предприятий в области защиты от внутренних и внешних угроз безопасности информации.

3. Регулирование интернет-контента: законодательство расширило возможности правительства в области блокировки и удаления интернет-контента, расцененного как необходимого к запрету, что способствует дальнейшему развитию безопасности интернет-среды на территории Индии.

Следующим значимым шагом Индийского правительства становится подписание соглашения с Соединенными Штатами Америки о кибербезопасности (2011 г.). Меморандум о взаимопонимании (Memorandum of Understanding) направлен на сотрудничество, обмен опытом и информацией между организациями соответствующих государственных отделов, ответственных за кибербезопасность. Соглашение в рамках американо-индийского стратегического диалога, начатого в 2009 г., было призвано выполнить обоюдное обязательство стран по укреплению глобальной безопасности и совместному противодействию терроризму. Благодаря этому соглашению соответствующие правительства и узконаправленные сообщества по кибербезопасности как в США, так и в Индии получали возможность вести скоординированные действия со своими коллегами относительно широкого диапазона технических и оперативных проблем. Основным действующим органом со стороны Индии стал вышеупомянутый CERT-IN.

Отдельным этапом выступает Национальная политика в области кибербезопасности, утвержденная правительством Индии в июле 2013 г. Это первый индийский доктринальный документ, обозначивший единое видение политических приоритетов государства, частного сектора и общества в целом в сфере кибербезопасности. Доктрина уделяет особое внимание оценке потенциальных рисков в данной области и развитию кадрового потенциала внутри страны.

Основные цели документа осуществляются благодаря следующим инициативам:

- создание Национального центра защиты критической информационной инфраструктуры (National Critical Information Infrastructure Protection Centre);
- создание Национального координационного центра по кибербезопасности (National Cyber Coordination Centre) в целях координации деятельности в данной сфере между различными правительственными учреждениями государства;
- выработка Национального плана исследований и разработок в области информационной безопасности;
- создание структуры для аудитов безопасности и сертификации продуктов и услуг информационной безопасности;
- разработка национального плана антикризисного управления для развития системы реагирования на киберинциденты внутри страны;
- повышение осведомленности о кибербезопасности среди населения и предприятий Индии [Mishra et al. 2016].

В рамках развития кадрового потенциала Индия привнесла такие новшества для своей страны, как, например, обучение национальной полиции посредством взаимодействия с Международным центром криминалистики и информационной безопасности (International Centre for Criminalistics and Information Security), проводя курсы для национальных органов правопорядка по борьбе с киберпреступностью.

Одним из важнейших пунктов национальной политики является учреждение Национального центра защиты критической информационной инфраструктуры (NCIIPC). Цель NCIIPC – принятие всех необходимых мер для содействия защите информационной инфраструктуры от любого вида нежелательного воздействия. NCIIPC как узловое учреждение защищает и предоставляет рекомендации по снижению уязвимости к кибертерроризму и другим глобальным угрозам цифрового пространства[15].

В настоящее время в Индии не существует всеобъемлющего агентства по информационной безопасности, подобного европейскому ENISA (Агентство Европейского союза по кибербезопасности), действующему с 2005 г. Однако в дополнение к CERT-IN и NCIIPC индийское правительство учредило Секретариат Совета национальной безопасности в качестве центрального координационного органа по кибербезопасности и управлению Интернетом. Он направлен на защиту киберпространства, включая критически важную информационную инфраструктуру, от атак, повреждений, неправомерного использования и экономического шпионажа.

В целом принятие национальной политики кибербезопасности привело к улучшению состояния данной области в Индии, к росту профессионализма и компетентности. Политика 2013 г. остается действующей доктриной Индии и по сей день, однако она была

[15] NCIIPC Framework for Evaluating Cyber Security in critical information infrastructure. 2018. 32 p. URL: https://nciipc.gov.in/documents/Evaluating_Cyber_Security_Framework.pdf (accessed 16 Nov 2023).

признана устаревшей, и с 2023 г. Индийское правительство занято оформлением новой доктрины.

Период 2014–2017 гг. маркирует масштабное оживление Индии в международном сотрудничестве в сфере развития информационной безопасности. За этот промежуток различные индийские структуры заключают свыше тридцати соглашений различного вида в целях международного взаимодействия. Широкий список включает следующие государства: 2014 г. – Финляндия, Южная Корея; 2015 г. – Бразилия, Канада, Китай, Германия, Австралия (2015, 2017), Малайзия (2015, 2016), Сингапур (2015, 2016); 2016–2017 гг. – Бельгия, Франция, Япония, Кения, Россия, Сербия, Саудовская Аравия, Катар, Индонезия, Новая Зеландия, Швеция, Таиланд, Великобритания, ЮАР, Вьетнам, Узбекистан, Бангладеш, Португалия, США.

Итогами данного расширения деятельности для Индии стали 39 соглашений, направленных на сбор и обмен информацией в целях обеспечения соблюдения государственных и уголовных законов отрасли кибербезопасности (так называемые MLAT Agreements); 54 Меморандума о Взаимопонимании и совместных заявления, а также сформированы 10 новых структур в сотрудничестве с Индией, состоящие из стандартов, руководящих принципов и практик, способствующих защите критической инфраструктуры информационной безопасности (как создание в 2015 г. между Индией и Китаем механизма уровня министерств внутренних дел двух государств по вопросам киберпреступности).

Формирование обновленной доктрины информационной безопасности Индии

К 2020 г. страна не перестает быть крайне уязвимой в вопросах кибербезопасности, система продолжает требовать улучшения как технической, так и правовой базы. Наиболее красноречиво данное положение характеризуют следующие факты.

Например, в первой половине 2019 г. ни одна страна мира не подвергалась большему количеству кибератак, чем Индия. По данным индийской телекоммуникационной компании Subex, только в трехмесячный промежуток с апреля по июнь 2019 г. количество кибератак увеличилось на 22 %. В целом за 2019 г. страна потеряла около 5,6 млрд долларов из-за киберпреступлений.

В рамках первого полугодия 2020 г. Индия заняла 3 место в мире по числу регистраций кибератак, а в глобальном индексе кибербезопасности (2018) Индия заняла лишь 47 место в мире. В 1-м квартале количество кибератак в стране выросло на 37 % по сравнению с 4-м кварталом 2019 г. 66 % индийских компаний претерпели как минимум по одной атаке / краже данных за этот период; расходы 56 % местных компаний в графе IT-защиты возросли двукратно, превысив среднемировой уровень; более 82 % индийских компаний столкнулись с атаками программ-вымогателей [Prasad, Kumar 2022].

Ввиду сложившихся обстоятельств индийские власти признают действующую национальную политику от 2013 г. недееспособной для современных реалий. В августе 2020 г. премьер-министром Индии была анонсирована новая национальная стратегия кибербезопасности. Изначально на ее осуществление было выделено 5 трлн долларов. План все еще находится на завершающем этапе разработки и ожидает утверждения для полного вступления в силу, однако уже известны его основные направления.

Новая национальная политика будет весьма амбициозной и имеет целью охватить политическую, экономическую и техническую сферы. Стратегия направлена на обеспечение безопасности киберпространства, а также на объединение и укрепление в значительной степени разрозненных ИТ-структур Индии. Документ содержит 21 ключевой пункт.

После подписания закона новая стратегия станет законодательной основой для борьбы с возникающими угрозами кибербезопасности. Среди ключевых пунктов доктрины стоит отметить увеличение заинтересованности Индии в международном взаимодействии, участии в глобальных мероприятиях, наращивании кадрового потенциала, сокращении нужд страны в квалифицированных специалистах. Увеличивается внимание к повышению осведомленности в отношении безопасности в сети всех слоев населения, стимулирования инвестиций в развитие технологий кибербезопасности, учебной инфраструктуры, демонстрации возможностей Индии на мировом рынке.

В целом доктрина предлагает серьезный пересмотр приоритетов по отношению к проблеме виртуальных угроз. Крайний элемент развития концепции информационной безопасности Индии к маю 2023 г. находился в разработке. Правительство рассматривает замену основного законодательного акта, регулирующего сферу информационных технологий в стране уже более 20 лет. На смену закону об ИТ готовится закон «О цифровой Индии», большой частью которого среди широкого списка других аспектов будет и кибербезопасность. Лицом, отвечающим за подготовку законопроекта, является государственный министр по электронике и информационным

https://doi.org/10.21603/sibscript-2024-26-3-441-458

технологиям Раджив Чандасекар. На сегодняшний день сроков по завершению подготовки и принятию нововведений нет, проекту еще предстоит претерпеть ряд изменений, слушаний и заседаний, однако уже сейчас можно сказать, что он точно станет значительной вехой для Индии.

Современная структура органов информационной безопасности

К данному моменту деятельность многих учреждений и государственных органов непосредственно регулирует сферу информационной безопасности. В административном плане обеспечение кибербезопасности возложено на Министерство электроники и информационных технологий (MeitY). Министерство пропускает через себя огромное количество решений и нововведений. Основные направления деятельности: участие в вопросах, касающихся законов о кибербезопасности, применение Закона об информационных технологиях от 2000 г., создание и корректировка национальных планов и стратегий развития концепции информационной безопасности, создание методических рекомендаций для населения.

Группа реагирования на компьютерные чрезвычайные ситуации CERT-IN, будучи подразделением MeitY, является основным агентством по борьбе с угрозами кибербезопасности. На группу реагирования возложена задача администрирования самого главного и всеобъемлющего законодательства Индии в области ИТ – IT Act 2000 г. (включая правки 2008 г.), в котором содержатся все статьи преступлений и соответствующих наказаний за них. CERT-In ведет деятельность по ряду ключевых направлений: от сбора данных, анализа киберугроз и уязвимостей и определения надлежащих мер их снижения вплоть до непосредственного реагирования на инциденты (включая судебную экспертизу и координацию дальнейшего разбирательства по делу). На правах вышестоящего национального агентства обо всех случаях правонарушений сферы информационных технологий и каких-либо других нежелательных ситуациях должно быть доложено в CERT-In (в течение 6-часового срока после происшествия). Группа реагирования предоставляет возможность любому пострадавшему от того или иного вида киберпреступления обратиться к ним в круглосуточном формате. Структура занимается информированием общественности о новейших уязвимостях системы информационной безопасности для пользователей среди населения и контрмерах по борьбе с ними, распространением информации об опасностях, создаваемых любого вида массовыми хакерскими атаками (к примеру, бум фишинговых сайтов в апреле 2013 г.).

В министерстве еще есть две примечательные инициативы: Кибер Суракшит Бхарат (Cyber Surakshit Bharat – CSB) и Кибер Свахта Кендра (Cyber Swachhta Kendra – CSK)[16]. Cyber Surakshit Bharat – это первое в своем роде государственно-частное партнерство, призванное использовать опыт ИТ-индустрии в области кибербезопасности. Запущенный в 2018 г. проект нацелен на распространение осведомленности о киберпреступности на территории Индии и мерах обеспечения безопасности. В рамках этой программы в сотрудничестве с такими мировыми гигантами, как MicroSoft, IBM и Intel, проводятся обучения для директоров по информационной безопасности и технических должностных лиц на самых высоких уровнях: центрального правительства, правительств штатов, банков государственного сектора, силовых структур обороны и технических подразделений ВВС, армии и флота страны.

В свою очередь CSK – это центр очистки так называемых ботнетов (способ контроля устройства извне) и анализа вредоносного программного обеспечения, он является частью видения индийского правительства государственного проекта «Цифровая Индия». Эта инициатива позволяет населению защитить свои смартфоны, ноутбуки и персональные компьютеры от кибератак. Находясь под управлением CERT-In, центр работает в сотрудничестве с интернет-провайдерами и антивирусными компаниями.

Однако и другие правительственные органы занимаются кибербезопасностью и смежными вопросами. Так, Министерство внутренних дел страны принимает в этом немалое участие – отдел кибербезопасности и информационной безопасности (C&IS) Министерства контролирует реализацию национальной политики и руководящих принципов информационной безопасности (NISPG) и имеет в своем составе отделы киберпреступности, кибербезопасности, информационной безопасности и отдел постоянного мониторинга происшествий. Отделом ведется деятельность по внедрению национальной разведывательной сети (NAGTRID) – структуры баз данных разведывательных организаций в целях борьбы с терроризмом, которая объединяет в себе информацию различных правительственных органов Индии. По своей сути,

[16] Cyber Swachhta Kendra. URL: https://www.csk.gov.in (accessed 16 Nov 2023).

NATGRID служит мерой распознания лиц, подозреваемых в терроризме (в том числе кибертерроризме), на территории страны.

Индийский координационный центр по борьбе с киберпреступностью (I4C), созданный по инициативе Министерства внутренних дел[17], ведет борьбу с киберпреступностью, координируя работу с полицией штатов всей страны. Запущенный в октябре 2018 г. центр I4C предназначен для предотвращения неправильного использования киберпространства в интересах экстремистских и террористических групп. Также он выступает как механизм, координирующий всю деятельность, связанную с осуществлением договоров о взаимной правовой помощи (MLAT) с другими странами (в области информационной безопасности). Его структура включает в себя национальное подразделение по анализу угроз кибербезопасности (TAU), которое представляет собой платформу для совместной работы сотрудников и специалистов правоохранительных органов, представителей частного сектора, научных кругов, исследовательских организаций. В координационный центр входит национальный учебный центр по киберпреступности (NCTC). Его цель состоит в стандартизации учебной программы курсов, посвященных кибербезопасности, проведении общедоступных тренингов и разработке массового открытого онлайн-курса, который будет проводиться на бесплатной свободно доступной учебной платформе.

Еще один ключевой отдел I4C – Национальный центр кибернетических исследований и инноваций, служащий мониторинговым центром новых технологических разработок. В его обязанности входит прогнозирование потенциальных уязвимостей и создание стратегических партнерств в области исследований и инноваций, ориентированных на борьбу с преступностью.

Стоит обратить внимание на орган регулирования и развития страхования (IRDAI). Его усилиями 9 октября 2022 г. была представлена улучшенная система информационной безопасности. Она направлена на побуждение страховых компаний к разработке надежного плана оценки рисков, расширению возможности предотвращения внутренних и внешних угроз, предотвращению любого вида мошенничества.

Важным механизмом регулирования со времени своего создания в 2006 г. выступает Апелляционный суд по киберрегулированию (CRAT). На правах руководящего органа он существует для вынесения решений по спорным ситуациям правонарушений. Суд предоставляет платформу для разрешения прецедентов киберпреступности с электронными транзакциями и цифровыми подписями.

Орган регулирования телекоммуникаций Индии (TRAI) вместе с Департаментом телекоммуникаций (DoT) послужили механизмом ужесточения правил конфиденциальности пользовательских данных и способов их использования. TRAI – как самостоятельный регулирующий орган, а DoT – в качестве исполнительного отдела Министерства связи. Учреждения работают в тандеме, чтобы регулировать сеть телефонных операторов и поставщиков услуг отрасли. Ими подготовлены рекомендации для операторов связи по теме «Конфиденциальность, безопасность и право собственности на данные в телекоммуникационном секторе». Документация затрагивает новые обязанности, связанные с данными о потребителях, в целях усиления защиты. Со стороны DoT ведется дополнительная деятельность по регулярному проведению семинаров и учений по кибербезопасности в интересах повышения осведомленности населения. Также они занимаются обработкой отчетов телекоммуникационных компаний страны по отслеженным вторжениям, атакам и мошенническим действиям.

В финансовой отрасли Индии имеются специальные механизмы. Инициатива KYC (Know Your Customer, или же «Знай своего клиента») – это обязательная стандартизированная на мировом уровне практика, в том числе предписанная Резервным банком Индии (RBI), гарантирующая клиентуре защиту их цифровой личности и данных о платежных операциях[18].

На территории Индии с 2012 г. действует крайне обширный проект Aadhaar – крупнейшая в мире биометрическая система. К марту 2016 г. правительством был принят закон, утверждавший работу государственных программ с Aadhaar. Aadhaar оказывает содействие в борьбе с мошенничеством в информационном пространстве и служит ключевым инструментом проверки подлинности личности пользователей в различных областях, включая банковское дело, социальную

[17] Cyber and Information Security (C&IS) Division. *Ministry of Home Affairs*. URL: https://www.mha.gov.in/en/divisionofmha/cyber-and-information-security-cis-division (accessed 16 Nov 2023).

[18] Cyber Regulation Apellate Tribunal. *The inact one*. 8 Apr 2023. URL: https://theintactone.com/2023/04/08/cyber-regulation-appellate-tribunal/ (accessed 16 Nov 2023).

https://doi.org/10.21603/sibscript-2024-26-3-441-458

защиту и налоговый сектор. Однако Aadhaar еще не дошел до идеального состояния. Система стала предметом нежелательного вида обсуждений, когда появилось несколько случаев утечки данных пользователей. Правительство Индии предпринимает шаги для усиления безопасности структуры Aadhaar.

Инструменты обеспечения информационной безопасности от внешних угроз

В первую очередь страна позаботилась о своей экономической безопасности в глобальном информационном пространстве. Действующая доктрина «Цифровой Индии» имеет определяющее значение в этом процессе. Суть ее состоит в полном переходе страны на цифровую экономику. И хотя Индия уже является одной из наиболее оцифрованных стран, демонстрируя показатели в более чем 1 млрд смартфонов и более 700 млн пользователей Интернета на территории государства, такой шаг становится логичным продолжением[19]. Цифровая экономика Индии приносит свои плоды уже сейчас, генерируя около 200 млрд долларов США от сектора информационных технологий: благодаря выручке от финансовых услуг с использованием информационных технологий, электронной коммерции и онлайн-платежей.

Но система, опирающаяся на бесперебойную работу цифровой инфраструктуры, сильно зависит от устойчивости взаимосвязей сетей и систем на всей территории страны. В связи с этим информационная безопасность становится ключевым фактором, обеспечивающим стабильность и благоприятные условия для дальнейшего развития экономической отрасли Индии.

Занимая первые позиции рейтингов наиболее атакуемых государств в глобальном киберпространстве, Индия постоянно находится в положении риска. Любая кибератака экономики страны будет иметь комплексные последствия. Широкий переход на цифровизацию приводит к увеличению объемов хранения и использования данных, в том числе критически важной и конфиденциальной информации. Но данные пополняются, а потенциальный риск растет вместе с ними.

В связи с этим за последнее десятилетие было предпринято несколько конкретных шагов в сторону предотвращения, раннего обнаружения и уменьшения негативного эффекта от киберугроз.

Информационная защита банковского сектора

В качестве одного из ключевых учреждений государства выступает Резервный банк Индии. В первую очередь под ответственность RBI попадает банковское управление. Резервный банк занимается разработкой и реализацией стратегии по защите национальных интересов в сфере информационной безопасности, включая защиту национальной валюты и финансовой системы. Руководящие принципы RBI предписывают, что он имеет право в произвольный момент запросить проверку киберустойчивости любого банка на территории страны (государственного или частного) – «Экспертизу кибербезопасности и информационных технологий»[20] (CSITE). Данная проверка проводится регулярно при Департаменте банковского надзора для периодической оценки прогресса, достигнутого банками во внедрении наиболее действенных мер кибербезопасности. Необходимость отчетности совокупности индийских банков помогает поддерживать планку качества экономической безопасности государства.

В 2018 г. деятельность банка расширяется с выходом закона «О резервном банке Индии» (RBI 2018). RBI в рамках новой доктрины формирует руководство по информационной безопасности для экономического сектора. В его документацию входят: распоряжения по регулированию электронного банкинга, управлению рисками и предотвращению кибермошенничества, проведению кризисного управления в критических ситуациях внешних атак, обеспечению безопасных электронных платежей и транзакций. RBI выпустил руководство по регулированию платежных агрегаторов и платежных шлюзов. В составе рекомендаций содержится предписание, согласно которому платежные агрегаторы обязуются внедрять механизм для мониторинга, обработки и отслеживания инцидентов и нарушений кибербезопасности, сообщать об инцидентах в RBI и CERT-In в целях их разрешения. Учреждения экономического сектора Индии также внедряют новейшие стандарты шифрования и безопасности транспортных каналов международной торговли.

Центральный банк обязывает банки следовать последним стандартам безопасности международного уровня ISO/IEC 27001 и ISO/IEC 27002[21]. Аналогичная структура была применена и к небанковским

[19] Analysing India's Economic Security Challenges. Jun 2022. № 32. 30 p. URL: https://www.gatewayhouse.in/wp-content/uploads/2022/06/Analysing-Indias-Economic-Security-Challenge.pdf (accessed 15 Nov 2023).

[20] Global Cybersecurity Index 2020…

[21] Analysing India's Economic Security Challenges…

финансовым компаниям. В состав законопроекта 2018 г. входит пункт, согласно которому банки должны следовать всем прописанным в законе рекомендациям, чтобы стандартизировать основы кибербезопасности обработки платежей и бороться с трудностями в современной цифровой среде. В случае несоблюдения закона RBI налагает штрафы на банки и другие учреждения финансового сектора.

На сегодняшний день в Индии ведется работа по разработке нового независимого учреждения по регулированию экономической безопасности в киберпространстве с промежуточным названием CERT-Fin (Группа реагирования на компьютерные чрезвычайные ситуации в финансовом секторе)[22]. Идея министерства финансов предназначена для снижения нагрузки с главного регулятора финансового сектора в лице RBI и основной группы реагирования CERT-In в непосредственном взаимодействии с вышеупомянутыми структурами.

Основу обязанностей CERT-Fin будет составлять анализ инцидентов кибербезопасности в экономическом секторе, координация действий по реагированию и изучение моделей внешних и внутренних угроз. Структура органа по первичной задумке должна быть узловой и включать в себя сеть небольших отраслевых групп реагирования в разных секторах экономики страны, каждая группа должна быть прикреплена к соответствующему регулирующему органу или крупной финансовой организации.

В свете обострения кибератак на Индийскую инфраструктуру после сезона пандемии COVID в 2020 г. создание такого учреждения приобретает особое значение. После пандемии индийские организации сообщали о вдвое большем количестве кибератак ежедневно. Необходимость в дополнительном регулировании стала очевидной, и CERT-Fin готовится стать ответом на новые вызовы.

До момента создания CERT-Fin он разрабатывал программное обеспечение и информационные системы для финансовых учреждений страны с целью обеспечения защищенности от внешних угроз глобального цифрового пространства. Наряду с этим Институт развития и исследований в области банковских технологий (IDRBT) ведет консультационные программы для организаций экономического сектора по безопасности на всей территории Индии.

Помимо того, рекомендационной деятельностью занимается и Совет по безопасности данных Индии (DSCI). Совет периодически выпускает рекомендационные сводки по усилению мер безопасности. В свете крупномасштабных атак в 2018 и 2020 г., нацеленных на малые, средние и крупные предприятия, DSCI выпустил руководство по предотвращению фишинговых атак злоумышленников на индийские организации. DSCI также предоставил информацию о мерах по смягчению неблагоприятных последствий нарушений экономической безопасности.

Свои регулятивные механизмы есть и в экономическом секторе ценных бумаг. Совет по ценным бумагам и биржам Индии (SEBI) выпустил подробные инструкции для учреждений рыночной инфраструктуры по созданию своего операционного центра кибербезопасности (Cyber Security Operation Centre). SEBI, взаимодействуя с другими агентствами, в том числе с CERT-In, национальным координационным центром кибербезопасности и Министерством MeitY, внедрил руководящие принципы. Они применялись к организациям, входящим в сферу деятельности Совета: фондовым брокерам, фондовым биржам, компаниям по управлению активами и другим видам организаций. Основные их цели: установление безопасности проведения операций как на территории Индии, так и с зарубежной клиентурой; усиление мер защищенности информационных систем указанных учреждений.

Шесть основных членов комитета SEBI следят за руководством инициативами в области кибербезопасности, наряду с консультацией по вопросам разработки и поддержания требований безопасности в соответствии с глобальными отраслевыми стандартами.

Международное взаимодействие Индии по проблемам информационной защиты

Международное взаимодействие Индии в интересах усиления своей защищенности и минимизации потенциальных врагов в глобальном информационном пространстве стоит выделить отдельно. Ключевыми акторами выступают организации IAMAI (Индийская ассоциация интернета и мобильной связи) и NASSCOM (Национальная ассоциация компаний-разработчиков программного обеспечения и услуг). Их представители принимают участие в международных форумах, конференциях и миссиях.

Ассоциация Интернета развивает спектр различных программ, предотвращающих киберугрозы

[22] Ibid.

https://doi.org/10.21603/sibscript-2024-26-3-441-458

для бизнес-секторов и защищающих интересы индийских компаний на мировых рынках. В рамках своей деятельности IAMAI содействует развитию интернет-экономики страны и ее безопасности, привлекая зарубежные инвестиции. NASSCOM работает над созданием благоприятной экономической среды для развития технологической индустрии и ее безопасного функционирования в глобальном информационном пространстве. NASSCOM регулярно представляет интересы индийского правительства и IT-компаний страны на международных форумах и организациях, таких как Всемирная торговая организация (ВТО) и Конференция ООН по торговле и развитию (UNCTAD). Ассоциация также стабильно участвует в разработке глобальных стандартов и регуляций.

Правительство Индии заинтересовано в максимально возможном расширении базы обмена информацией, для чего заключает ряд соглашений в глобальном пространстве. Наиболее важными направлениями сотрудничества являются США, Израиль и Южная Корея.

Соглашение между Индией и США было подписано в 2016 г. Оно регулировало формирование цифровой экономики, привносило принципы совместной работы по развитию и применению новых технологий и обмену стратегически важной информацией о возможных киберугрозах и методах борьбы с ними.

Отношения с Израилем закреплены в меморандуме 2018 г., регламентирующем укрепление сотрудничества учреждений двух стран путем создания общих стартапов и ведения совместной деятельности по организации инновационных проектов. Значимую роль сотрудничества с Израилем играет обмен информацией и отчетностью как государственных, так и независимых органов, регулирующих киберпространство.

Взаимодействие с Южной Кореей осуществляется на основе заключенного в 2019 г. совместного заявления о сотрудничестве. Соглашение включало обязательный для международного партнерства пункт индийского правительства об организации обмена информацией в области безопасности. С момента вступления заявления в силу совместно с Кореей регулярно проводятся учения для специалистов отрасли, организуются двухсторонние конференции по предотвращению различного рода атак на цифровое пространство стран-партнеров, поднимаются вопросы о коллаборациях в разработке и совершенствовании новых директив безопасности финансовых систем.

Индия является одной из лидирующих стран по экспорту информационных технологий, аутсорсингу IT-задач и ряду других направлений. Такая высокая активность в совокупности с огромным рынком Индии вызывает острую необходимость в постоянном развитии информационной безопасности.

Регулярно сталкиваясь с внешними угрозами безопасности базам данных, Индия считается привлекательной целью для иностранного вмешательства, например различного рода хакерские атаки (фишинг, взлом паролей государственных деятелей, эксплойты уязвимостей программного обеспечения или ряд других методов). Государственный аппарат на постоянной основе предпринимает шаги по борьбе с этими рисками в попытках надежнее обезопаситься и не дать зарубежным недоброжелателям получить доступ к системам критически важных баз данных.

Заключение

Для защиты информации в глобальном информационном пространстве Индия принимает меры на разных уровнях: от создания самостоятельных организаций до продвижения новейших технических решений. И хоть в настоящее время ответом страны на вызовы безопасности должна стать новая национальная стратегия, которая еще находится в состоянии подготовки и усовершенствования, страна все равно имеет необходимую базу регуляций.

В документации Министерства электронной связи и информационных технологий список критических областей, требующих информационной защиты, представлен следующими секторами: энергетика, банковские и финансовые услуги, страхование, телекоммуникации и связь, транспорт, правительственный сектор, государственные предприятия.

Для секторов критической важности правительство создало Национальный центр защиты критической информационной инфраструктуры (NCIIPC) при IT Act в качестве узлового агентства[23]. Он является государственным институтом в вопросах внешней защиты от несанкционированного доступа, изменения, незаконного использования, раскрытия и сбоев

[23] The Information Technology Act, 2000. *Ministry of Law, Justice and Company Affairs (Legislative Department)*. New Delhi, 9 Jun 2000. URL: https://eprocure.gov.in/cppp/rulesandprocs/kbadqkdlcswfjdelrquehwuxcfmijmuixngudufgbuubgubfugbububjxcgfvsbdihbgfGhdfgFHytyhRtMjk4NzY= (accessed 16 Nov 2023).

в работе. NCIIPC обеспечивает повышение защиты и устойчивости критической информационной инфраструктуры за счет проведения обязательных процедур и методов обеспечения безопасности.

NCIIPC предоставил рекомендации, направленные на снижение уровня уязвимости CII к глобальным угрозам кибертерроризма, кибервойн и других, менее серьезных потенциальных опасностей. Официальные рекомендации организации основаны на длительном процессе тщательного мониторинга, сбора, анализа и прогнозирования угроз киберпространства на национальном уровне.

NCIIPC в рамках своей деятельности является и международным актором. В сферу заинтересованности Национального центра за рубежом входит проведение совместных с иностранными коллегами исследований и разработок, финансирование проектов по созданию и развитию инновационных технологий. В целях усовершенствования защиты критически важных баз данных проводится тесное сотрудничество с международными партнерами. Так, представители NCIIPC принимают участие в конференциях, семинарах и другого рода массовых мероприятиях, в том числе в заседаниях ООН и международного союза электросвязи (ITU), направленных на обмен опытом, передачу стратегических знаний и обучение кадров. Важным аспектом работы центра является разработка и реализация национальных и международных стратегий сотрудничества, на которые правительство Индии опирается в формировании соглашений с потенциальными зарубежными партнерами в целях укрепления своих позиций на глобальной информационной арене.

Как итог, Индия подписала договоры о взаимной помощи почти с 35 странами для продуктивного сотрудничества в отношении развития регуляции защиты доступа к базам данных как государственного, так и частного сектора. Среди наиболее важных партнерских отношений выделяются США, Великобритания, Япония и Франция.

В 2018 г. центральное правительство Индии принимает новый нормативный акт – «Правила по практике и процедурам информационной безопасности для защищенной системы». Документ содержит подробные инструкции по управлению и конфигурации защищенных систем, контролю и мониторингу действий пользователей информации в защищенных структурах. Большое внимание уделяется защите от кибератак и вредоносных программ, поступающих извне и составляющих угрозу национальной безопасности.

Кроме того, стоит отметить, что с августа 2021 г. правительство Индии утвердило обновленную схему работы некоторых подгрупп центра NCIIPC, постепенно внедряя использование искусственного интеллекта. Это поможет организациям и компаниям достигать целей более эффективно и в ускоренные сроки.

В поддержку MeitY и Национальному центру защиты критической информационной инфраструктуры была учреждена новая организация, получившая название Секретариат Совета национальной безопасности (NSCS)[24] (п. 1.2). В целях координации действий в аспекте безопасности информационного пространства секретариат работает в тесном взаимодействии с Министерством внутренних дел, Министерством обороны, Министерством иностранных дел, разведывательным отделом Индии и др. Секретариат ведет разработку проекта национальной стратегии кибербезопасности. Секретариат Совета национальной безопасности также ведет деятельность в сотрудничестве с международными организациями и структурами других государств в вопросах национальной безопасности критических баз данных страны.

В ноябре 2019 г. было создано Агентство обороны по кибербезопасности (Defence Cyber Agency, DCA), которое возглавил контр-адмирал военно-морского флота Индии Мохит Гупта [Mishra et al. 2016]. Заинтересованность страны в усилении безопасности цифрового военного сектора обуславливалась увеличением количества киберугроз. В качестве основных источников угроз выступали Китай, Пакистан и Соединенные Штаты Америки [Mishra et al. 2016].

Китай на протяжении длительного времени является главным конкурентом Индии в глобальном киберпространстве, их хакерские атаки чаще всего нацеливались на кражу данных из ресурсов государственных баз, конфиденциальных данных значимых национальных и частных учреждений. Действия Пекина можно было расценивать как полноценную кибервойну в отношении Индии.

Пакистан в свою очередь является серьезным оппонентом Индии на южной границе. Пакистанские силы зачастую преследовали цели атаковать сайты

[24] NeGD, MeitY organises 30th Batch of Chief Information Security Officers' (CISOs) Deep Dive Training Programme under Cyber Surakshit Bharat Initiative. 3 Sep 2022. URL: https://pib.gov.in/PressReleasePage.aspx?PRID=1856472 (accessed 15 Nov 2023).

https://doi.org/10.21603/sibscript-2024-26-3-441-458

индийских правительственных учреждений и военных объектов, но угрозы Пакистана менее значительны.

С точки зрения взаимодействия с США положению дел было сложно дать однозначную оценку. На первый взгляд, страны связывало обоюдно продуктивное соглашение о взаимопомощи от 2016 г., в рамках которого проводились совместные учения и мероприятия по обмену опытом и новыми разработками. Но в то же время на фоне ухудшающихся отношений в общественно-политической сфере спецслужбами США излагались интересы навязывания своей модели кибербезопасности от внешних угроз.

За более чем двадцатилетний период Индия совершила серьезнейший скачок в отрасли информационных технологий как на внутреннем уровне, так и на мировой арене. С момента формирования первого свода законов, регулирующего цифровую сферу, государство планомерно развивало концепцию безопасности в информационном пространстве. Расширяя нормативную базу, вводя новые и новые учреждения различного статуса и предназначения, постоянно обновляя взгляд на национальную стратегию развития кибербезопасности, Индия удостоилась места в ряду наиболее значимых стран с точки зрения состояния цифровой структуры и ее защищенности. Государство прошло путь от обладателя одного из самых бедных и примитивных секторов информационно-коммуникационных технологий до закрепления своего места в строю мировых лидеров. Конечно, к сегодняшнему дню инфраструктура информационной безопасности страны неидеальна и требует значительных шагов вперед, находясь под перманентным прицелом хакерских атак. Однако путь ее формирования и отдельные примечательные инициативы являются значимым опытом, заслуживающим внимания мировых специалистов.

В ходе исследования было поэтапно описано формирование концепции информационной безопасности Индии. В качестве ключевых событий были взяты относящиеся к системе информационной безопасности страны. Среди стадий представлены: формирование и принятие нормативно-правовых актов отрасли; учреждение новых государственных и независимых органов, агентств и организаций, ведущих деятельность непосредственно в среде информационной безопасности или касающихся ее; принятие национальных доктрин (стратегий и национальных политик развития сектора); ключевые события в международном взаимодействии – заключение соглашений, пактов, меморандумов и т. д.

Были определены и более детально охарактеризованы механизмы, обеспечивающие информационную безопасность внутри Индии. В их список был включен ряд государственных учреждений. Ключевые позиции занимают отделы министерств страны. Таким образом, основные функции регулирования внутреннего киберпространства возложены на Министерство электроники и информационных технологий и его подразделение – группу реагирования на компьютерные чрезвычайные ситуации (CERT-IN). В списке также присутствуют учрежденные Министерством внутренних дел страны Отдел кибербезопасности и информационной безопасности (C&IS) и Индийский координационный центр по борьбе с киберпреступностью (I4C). Среди иных инициатив выделяются главенствующий свод законов отрасли – IT Act 2000 г. (включая поправки 2008 г.), правила 2011 г., акт «Знай своего клиента» и система Aadhaar.

С точки зрения защиты от внешних угроз были представлены основные механизмы, регулирующие позиции Индии в глобальном информационном пространстве. Данная категория была разделена на механизмы двух отраслей: концентрирующиеся на экономическом секторе и сфокусированные на защите данных страны. В ряду первых – Резервный (он же Центральный) банк Индии (RBI) и созданный им Институт развития и исследований в области банковских технологий (IDRBT), Совет по безопасности данных Индии (DSCI), организации IAMAI (Индийская ассоциация Интернета и мобильной связи) и NASSCOM (Национальная ассоциация компаний-разработчиков программного обеспечения и услуг).

Вторая половина представлена созданным правительством в 2014 г. Национальным центром защиты критической информационной инфраструктуры (NCIIPC), который выпустил в 2018 г. нормативный акт «Правила информационных технологий». Деятельность центра является основополагающей в секторе критически важной инфраструктуры Индии. Был отмечен вклад DCA (Агентство обороны по кибербезопасности) в усиление безопасности баз данных цифрового военного сектора и NSCS (Секретариат Совета национальной безопасности) как международного актора в вопросах национальной безопасности критических баз данных страны.

Данное исследование позволило достичь поставленную цель и предоставляет полную картину поэтапного выстраивания структуры информационной безопасности Индии. По последовательности их учреждения и вступления в силу были затронуты

https://doi.org/10.21603/sibscript-2024-26-3-441-458

все основные действующие и разрабатываемые механизмы обеспечения защиты киберпространства страны. Детально описаны их функции и цели, различного рода нормативно-правовые акты (от свода правил до национальных доктрин) и органы по регулированию описываемой сферы информационной безопасности. Предоставлен целостный взгляд на развитие концепции информационной безопасности внутри страны и за ее пределами, сконцентрированный на хронологическом повествовании о каждой стадии ее формирования. Информация изложена с конкретным разделением всех основных ныне присутствующих в стране механизмов на отдельные группы. Процесс создания инфраструктуры информационной безопасности Индии представлен с четким подразделением рассматриваемых событий и инициатив на конкретные категории.

Подводя итог, стоит отметить, что Индия, несмотря на огромный перечень преград и угроз, построила надежную систему информационной безопасности, отвечающую современным мировым запросам. Согласно Global Cybersecurity Index 2020 г., Индия занимает 15 место по уровню кибербезопасности в международном рейтинге, что безусловно является отличным результатом [Reghunadhan 2022: 25]. Государство своевременно реагировало на мировые тенденции в глобальном информационном пространстве, внедряя необходимые механизмы регулирования. К данному моменту в Индии ведут свою деятельность ряд ключевых учреждений в каждой из значимых отраслей кибербезопасности страны, сформирована нормативно-правовая база для предотвращения и борьбы с киберугрозами извне. Но при этом Индия остается в списке наиболее атакуемых в цифровом пространстве стран, что стимулирует правительство на дальнейшее развитие отрасли и привнесение стратегически важных инноваций в сектор, а также обновление общенационального курса совершенствования сферы информационных технологий в виде ожидаемой новой стратегии кибербезопасности страны.

В перспективе дальнейших исследований специалистов в области международных отношений информационной безопасности остается ряд вопросов о том, как будет национальная стратегия информационной безопасности Индии увязана с союзническими обязательствами по раскрытию ряда аспектов информации и обеспечению ее транспарентности, сбором данных в центре, которым, наверняка, станет Пентагон, в составе QUAD.

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

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

Литература / References

Авешникова А. А. Правовое обеспечение информационной безопасности несовершеннолетних в Индии. *Евразийский юридический журнал*. 2018. № 11. С. 55–57. [Aveshnikova A. A. Legal provision of information security of minors in India. *Evraziiskii iuridicheskii zhurnal*, 2018, (11): 55–57. (In Russ.)] https://elibrary.ru/vorbnr

Бухарин В. В. Кибербезопасность БРИКС. *Государственное управление Российской Федерации: повестка дня власти и общества*: XVI Междунар. конф. (Москва, 31 мая – 2 июня 2018 г.) М.: КДУ, 2019. С. 552–559. [Bukharin V. V. Cybersecurity of the BRICS. *Public administration of the Russian Federation: Agenda of authorities and society*: Proc. XVI Intern. Sci.-Prac. Conf., Moscow, 31 May – 2 Jun 2018. Moscow: KDU, 2018, 552–559. (In Russ.)] https://elibrary.ru/ylenpg

Дементьев О. М., Яркин М. С. Регулирование кибербезопасности в Индии. *Проблемы борьбы с киберпреступлениями в современном обществе*: II Всерос. конф. (Тамбов, 24 апреля 2017 г.) Тамбов: Изд-во Першина Р. В., 2017. С. 83–87. [Dementiev O. M., Yarkin M. S. Cybersecurity regulation in India. *Problems of combatting cybercrime in modern society*: II All-Russian Conf., Tambov, 24 Apr 2017. Tambov: Izd-vo Pershina R. V., 2017, 83–87. (In Russ.)] https://elibrary.ru/xfmddc

Замулина А. Опыт Страны цветущего лотоса. Регулирование сферы персональных данных в Индии. *BIS Journal – Информационная безопасность банков*. 2023. № 2. С. 94–97. [Zamulina A. Experience of the Land of the Blooming Lotus. Regulation of personal data in India. *BIS Journal*, 2023, (2): 94–97. (In Russ.)]

Зиновьева Е. С., Игнатов А. А. БРИКС в глобальном режиме ИКТ-безопасности. *Международные процессы*. 2023. Т. 21. № 4. С. 104–132. [Zinovieva E. S., Ignatov A. A. The role of BRICS in the international ICT security regime. *Mezhdunarodnye Protsessy*, 2023, 21(4): 104–132. (In Russ.)] https://doi.org/10.17994/IT.2023.21.4.75.2

Казарин О. В., Тарасов А. А. Современные концепции кибербезопасности ведущих зарубежных государств. *Вестник РГГУ. Серия: Документоведение и архивоведение. Информатика. Защита информации и информационная безопасность*. 2013. № 14. С. 58–74. [Kazarin O. V., Tarasov A. A. Modern concepts of cybersecurity of leading foreign countries. *Vestnik RGGU. Seriia: Dokumentovedenie i arkhivovedenie. Informatika. Zashchita informatsii i informatsionnaia bezopasnost*, 2013, (14): 58–74. (In Russ.)] https://elibrary.ru/rlygmt

Маланичева Н. В., Харина О. А., Балаханова Д. К., Великороссов В. В. Особенности концепции национальной безопасности Индии. *Прикладные экономические исследования*. 2023. № 2. С. 39–49. [Malanicheva N. V., Kharina O. A., Balakhanova D. K., Velikorossov V. V. Pecularities of India's national security concept. *Applied economic research*, 2023, (2): 39–49. (In Russ.)] https://doi.org/10.47576/2949-1908_2023_2_39

Михайлова Е. В., Горбунова О. А. Сравнительная характеристика финансовых рынков стран БРИКС. *Вестник евразийской науки*. 2019. Т. 11. № 2. [Mikhaylova E. V., Gorbunova O. A. Comparative characteristics of financial markets of the BRICS countries. *The Eurasian Scientific Journal*, 2019, 11(2). (In Russ.)] URL: https://esj.today/PDF/85ECVN219.pdf (дата обращения: 15.11.2023). https://elibrary.ru/dmznjv

Никипорец-Такигава Г. Ю., Бучнев Е. В., Харина О. А., Алексеева Ю. Н. Российско-индонезийское сотрудничество в сфере обеспечения кибербезопасности. *Юго-Восточная Азия: актуальные проблемы развития*. 2023. Т. 3. № 2. С. 84–95. [Nikiporets-Takigawa G. Yu., Buchnev E. V., Kharina O. A., Alekseeva Yu. N. Cooperation between Russia and Indonesia: A cybersecurity perspective. *YugoVostochnaya Aziya: aktual'nyye problemy razvitiya*, 2023, 3(2): 84–95. (In Russ.)] https://doi.org/10.31696/2072-8271-2023-3-2-59-084-095

Перминов В. А. Развитие сектора ИКТ в Индии. *Российский внешнеэкономический вестник*. 2019. № 8. С. 127–134. [Perminov V. A. Development of ICT sector in India. *Rossijskij vneshnejekonomicheskij vestnik*, 2019, (8): 127–134. (In Russ.)] https://elibrary.ru/pxoivx

Ревенко Л. С., Ревенко Н. С. Международная практика реализации программ развития цифровой экономики: примеры США, Индии, Китая и ЕС. *Международные процессы*. 2017. Т. 15. № 4. С. 20–39. [Revenko L. S., Revenko N. S. Global trends and national specifics of the development of a digital economy: Record of the Unites State, India, China and the EU. *Mezhdunarodnye Protsessy*, 2017, 15(4): 20–39. (In Russ.)] https://doi.org/10.17994/IT.2017.15.4.51.2

Сахаров В. С. Основная роль БРИКС, как международной организации, в борьбе с киберпреступностью. *Вестник Восточно-Сибирской Открытой Академии*. 2023. № 50. [Sakharov V. S. The main role of BRICS as an international organization in the fight against cybercrime. *Vestnik Vostochno-Sibirskoi otkrytoi akademii*, 2023, (50). (In Russ.)] URL: https://s.esrae.ru/vsoa/pdf/2023/50/1414.pdf (дата обращения: 15.11.2023). https://elibrary.ru/cktwox

Суюнова Ф. Б. Особенности цифровизации экономики Индии. *Oriental Renaissance: Innovative, Educational, Natural and Social Sciences*. 2022. Т. 2. № 9. С. 503–508. [Suyunova F. B. Digitalization of Indian economy. *Oriental Renaissance: Innovative, Educational, Natural and Social Sciences*, 2022, 2(9): 503–508. (In Russ.)]

Bhattacharjee S. An evolving paradigm of cybersecurity in North Eastern India. *Sustainable development goals in Northeast India*, eds. Anand S., Das M., Bhattacharyya R., Singh R.B. Singapore: Springer, 2023, 299–313. https://doi.org/10.1007/978-981-19-6478-7_16

Godse V. Building an ecosystem for cyber security and data protection in India. *Ethics and policy of biometrics. ICEB 2010. Lecture notes in computer science*, eds. Kumar A., Zhang D. Berlin, Heidelberg: Springer, 2010, 138–145.

ICT with intelligent applications: Proc. of ICTIS 2022, eds. Choudrie J., Mahalle P., Perumal T., Josh A. Singapore: Springer, 2022, vol. 1, 846. https://doi.org/10.1007/978-981-19-3571-8

Kumar V., Inbaraj P. Overview on cyber security threats involved in the implementation of smart grid in countries like India. *Proceeding of the International Conference on Computer Networks, Big Data and IoT (ICCBI – 2018). ICCBI 2018*, eds. Pandian A., Senjyu T., Islam S., Wang H. Cham: Springer, 2018, 678–684. https://doi.org/10.1007/978-3-030-24643-3_81

Lessambo F. I. AML / CFT and cybersecurity laws in India. *Anti-money laundering, counter financing terrorism and cybersecurity in the banking industry*. Cham: Palgrave Macmillan, 2023, 137–142. https://doi.org/10.1007/978-3-031-23484-2_14

Mishra S., Dhir S., Hooda M. A study on cyber security, its issues and cyber crime rates in India. *Innovations in computer science and engineering. Advances in Intelligent Systems and Computing*, eds. Saini H. S., Sayal R., Rawat S. S. Singapore: Springer, 2016, 249–253. https://doi.org/10.1007/978-981-10-0419-3_30

Patil S. India's cyber security landscape: Vulnerabilities and responses. *Securing India in the Cyber Era*, ed. Patil S. London: Routledge, 2021, 14–24. https://doi.org/10.4324/9781003152910

Patil S. India's cyber security landscape. Varying dimensions of India's national security. *India studies in business and economics*, eds. Behera A., Mishra S. Singapore: Springer, 2022, 75–90. https://doi.org/10.1007/978-981-16-7593-5_6

Prasad S., Kumar A. Cyber terrorism: A growing threat to India's cyber security. *Nontraditional security concerns in India*, eds. Singh S. K., Singh S. P. Singapore: Palgrave Macmillan, 2022, 53–73. https://doi.org/10.1007/978-981-16-3735-3_4

Reghunadhan R. *Cyber technological paradigms and threat landscape in India*. Singapore: Palgrave Macmillan, 2022, 134. https://doi.org/10.1007/978-981-16-9128-7

Shukla S. K., Agrawal M. *Cyber security in India: Education, research and training*. Singapore: Springer, 2020, 108. https://doi.org/10.1007/978-981-15-1675-7