КОМПОНЕНТЫ ЦИФРОВОГО СУВЕРЕНИТЕТА РОССИЙСКОЙ ФЕДЕРАЦИИ КАК ТЕХНИЧЕСКАЯ ОСНОВА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В.В. Бухарин

Факультет государственного управления, МГУ имени М.В. Ломоносова, 119991, Россия, Москва, ГСП-1, Ломоносовский проспект, д. 27, корп. 4.

В статье рассматривается возникновение в России понятия «информационный суверенитет», перспективы его практического и теоретического введения в научный оборот. Исследуется проблема «информационного суверенитета» в нормативных документах России, Китая и других стран. Основное внимание в статье, впервые в отечественной и зарубежной историографии, уделено техническому аспекту проблемы независимости в области цифровых технологий. В этой связи анализируются наиболее важные компоненты цифрового суверенитета, технически обеспечивающие национальную безопасность. Автор приходит к выводу, что основной отличительной особенностью российской технической базы по обеспечению информационного суверенитета является неравномерность и фрагментарность развития её компонентов. Наибольший прогресс достигнут в развитии таких компонентов как российские поисковые системы, социальные сети, национальный сегмент сети Интернет и навигационная система. Российское программное и аппаратное обеспечение требует ускоренного развития для обеспечения информационного суверенитета, национальной безопасности России. Наибольшего внимания заслуживает российская платёжная система, поскольку данный вопрос находится в прямой зависимости от направления развития экономики страны. Проблема обеспечения информационного суверенитета в значительной степени связана с вопросами принятия государственных решений, приведения нормативной, законодательной базы в соответствие с концепцией национальной безопасности страны.

Ключевые слова: информационный суверенитет, цифровой суверенитет, национальная безопасность, информационная безопасность, импортозамещение.

В процессе глобализации и интеграции появляются наднациональные органы управления, переформатируются национальные и международные институты. В научных и политических кругах всё более распространённым становится мнение о том, что государственный суверенитет, в традиционном понимании, утрачивает своё значение.

Для основоположника теории государственного суверенитета Ж. Бодена – государственного деятеля Франции, писателя и мыслителя эпохи Возрождения, суверенитет ассоциировался с верховной властью правителя. Соответственно, он являлся одним из главных признаков государства, его основой [4, с. 137, 151-158]. Именно независимые, суверенные государства на протяжении многих столетий играли ведущую роль в системе международных отношений. В отечественной историографии государственный суверенитет определяется как «верховенство и независимость государственной власти, проявляющиеся в соответствующих формах во внутренней и внешнеполитической деятельности государства» [5, с. 26].

В конце XX - начале XXI вв. существенно возросла роль информационных технологий и информационной сферы в целом, которая представляет собой «совокупность информации, информационной инфраструктуры, субъектов, осуществляющих сбор, формирование, распространение и использование информации, а также системы регулирования возникающих при этом общественных отношений»[1]. В связи с ограниченностью запасов сырьевых и энергетических ресурсов именно информация (знания), стала тем ресурсом, обладание которым даёт стратегические преимущества в конкурентной борьбе между странами, в мировой политике и международных отношениях. «Информационная сфера, являясь системообразующим фактором жизни общества, активно влияет на состояние политической, экономической, оборонной и других составляющих безопасности Российской Федерации»[2]. Развитие информационно-коммуникационных технологий (ИКТ) в условиях глобализации ведёт к появлению качественно новых (информационных) методов и технологий борьбы, которые могут принимать форму так называемых сетевых, кибер-, гибридных и информационных войн. Это требует поддержания своей государственной самостоятельности (суверенитета) на новом, информационном уровне.

Основной задачей исследования является изучение состояния компонентов цифрового суверенитета как технической основы информационной безопасности России, их влияния на национальную безопасность, а также анализ применения понятия «информационный суверенитет» в нормативных документах России и стран ближнего и дальнего зарубежья.

Согласно Доктрине информационной безопасности Российской Федерации, «интересы государства в информационной сфере заключаются в создании условий для обеспечения суверенитета и территориальной целостности России»[3], т.е. традиционного государственного суверенитета.

Понятия «цифровой» или «информационный суверенитет» [10], «суверенитет в информационном пространстве» - достаточно новые. До 2016 г. они фактически отсутствовали в российских нормативных документах. В науке не сложилось чёткой дефиниции данных терминов. Вызывает вопрос и их происхождение. В российском сегменте сети Интернет, авторство приписывается Н.Н. Федотову - главному аналитику компании InfoWatch, а одним из основных популяризаторов считается И.С. Ашманов - генеральный директор компании «Ашманов и партнёры». Компании тесно сотрудничают, являются одними из лидеров российских информационных технологий (IT). «Ашманов и партнёры» занимаются интернет-маркетингом, InfoWatch - информационной безопасностью в корпоративном секторе: защитой корпораций от утечек информации и целевых атак извне. На долю последней приходится около 50% российского рынка в области систем защиты конфиденциальных данных.

И.С. Ашманов одним из первых в России попытался дать определение «цифрового суверенитета», понимаемого как «право государства определять свою информационную политику самостоятельно, распоряжаться инфраструктурой, ресурсами, обеспечивать информационную безопасность и т.п. Цифровой суверенитет также можно поделить на несколько категорий. Одна из них – электронный суверенитет, который связан с защитой от кибератак»[4]. Как видно из определения, у Ашманова понятие «цифровой суверенитет» тождественно «информационному суверенитету».

Определение информационного суверенитета присутствует в нормативных документах некоторых стран ближнего и дальнего зарубежья. Например, в Законе Украины «О национальной программе информатизации» информационный суверенитет государства определяется как «способность государства контролировать и регулировать потоки информации из-за пределов государства в целях соблюдения законов Украи-

[1] Доктрина информационной безопасности Российской Федерации // Совет Безопасности Российской Федерации. [Электронный ресурс]. URL: http://www.scrf.gov.ru/documents/6/5.html (дата обращения: 07.10.2016).

[2] Там же.

[3] Там же.

[4] Ашманов И. Информационный суверенитет России: новая реальность // Россия навсегда. 13.05.2013. [Электронный ресурс]. URL: http://rossiyanavsegda.ru/read/948/ (дата обращения: 07.10.2016).

ны, прав и свобод граждан, гарантирования национальной безопасности государства»[5]. Согласно законодательству Украины, главным органом в системе центральных органов исполнительной власти в сфере обеспечения информационного суверенитета является Министерство информационной политики Украины, учреждённое постановлением Кабинета Министров Украины от 14 января 2015 г. № 2.

Понятие «суверенитет в информационной сфере» присутствует в законодательстве Белоруссии. Так, в «Стратегии развития информатизации в Республике Беларусь на 2016 – 2022 гг.» говорится о том, что необходимо «содействие обеспечению национального суверенитета в информационной сфере и национальной безопасности»[6]. В документе фигурирует также термин «цифровой суверенитет», определение которого отсутствует. Однако очевидно, что эти понятия не тождественны. В Стратегии подчеркивается, что «развитие национальной отрасли информационных технологий – необходимое условие успешного развития информатизации, обеспечения 'цифрового суверенитета' государства, а также важный фактор глобальной конкурентоспособности экономики страны». В качестве важной задачи отмечено, что необходима «организация научных исследований, разработка и производство собственных аппаратных и программных средств защиты информации, ключевых элементов ИКИ, совершенствование системы их стандартизации, сертификации и аттестации в целях обеспечения информационной безопасности и 'цифрового суверенитета' Республики Беларусь»[7].

В Китае с 2010 г. активно развивается так называемая концепция «интернет суверенитета», которая нашла отражение в «белой книге» под названием «Интернет в Китае»[8]. В работе «Мысли об интернет–суверенитете»[9] (опубликованной в 2015 г.) Е Чжен – члена Стратегического Консультативного комитета Народной Освободительной армии Китая -делается вывод о том, что «интернет-суверенитет» непосредственно влияет на национальную безопасность и стабильность. В его трактовке появление понятия «интернет–суверенитет» связано с переосмыслением Китаем «государственного суверенитета».

На работу Е Чжен оперативно отреагировала американская пресса. Джеймс Ареди на страницах The Wall Street Journal отметил, что «председатель КНР Си Цзиньпин с помощью консерваторов в правительстве, учёных, военных и использования высоких технологий стремится к тому, чтобы оказывать влияние на весь цифровой мир Китая, от полупроводников до социальных медиа»[10]. 23 мая 2016 г. Симон Деньер в The Washington Post опубликовал статью «Страшный урок Китая для мира: Цензура интернета работает»[11]. Содержание статьи полностью отражено в её заголовке.

Стоит отметить, что Китай действительно блокирует для своих граждан доступ к ресурсам, запрещённым китайским правительством. Система фильтрации контента, под названием «Золотой щит», более известная в западных СМИ как «Великий китайский файервол» (The Great Firewall of China) [19], была запущена в 2003 г. В её разработке принимали участие американские корпорации, в том числе и IBM.

Безусловно, существует достаточно простой, но весьма спорный способ поддержания информационного суверенитета: тотальный контроль и запрещение или ограничение части СМИ и сети Интернет. Так, Куба долгое время сохраняла свой информационной суверенитет во многом благодаря почти полному отсутствию доступа в интернет у населения.

В настоящее время Америка делает новые попытки проникнуть в информационное пространство Кубы. Несколько лет назад Агентство международного развития (АМР США) начало финансировать кубинскую версию Twitter - ZuneZuneo через кубинско-американскую мо-

[5] Закон Украины от 4 февраля 1998 года №74/98-ВР «О национальной программе информатизации» // WEB-версия ИПС «Законодательство стран СНГ». [Электронный ресурс]. URL: http://base.spinform.ru/show_doc.fwx?rgn=31607 (дата обращения: 07.10.2016).

[6] Стратегия развития информатизации в Республике Беларусь на 2016 – 2022 гг. // e-Gov.by. [Электронный ресурс]. URL: http://e-gov.by/zakony-i-dokumenty/strategiya-razvitiya-informatizacii-v-respublike-belarus-na-2016-2022-gody (дата обращения: 07.10.2016).

[7] Там же.

[8] The Internet in China. Information Office of the State Council of the People's Republic of China // China Internet Information Center. 8 June 2010. [Электронный ресурс]. URL: http://www.china.org.cn/government/whitepaper/node_7093508.htm (дата обращения: 07.10.2016).

[9] Bandursk D. China's Internet sovereignty // The China Media Project. [Электронный ресурс]. URL: http://cmp.hku.hk/2015/10/02/39285/ (дата обращения: 07.10.2016)

[10] Areddy J.T. China Pushes to Rewrite Rules of Global Internet // The Wall Street Journal. 28 July 2015. [Электронный ресурс]. URL: http://www.wsj.com/articles/china-pushes-to-rewrite-rules-of-global-internet-1438112980 (дата обращения: 07.10.2016).

[11] Denyer S. China's scary lesson to the world: Censoring the Internet works // The Washington Post. 23 May 2016. [Электронный ресурс]. URL: https://www.washingtonpost.com/world/asia_pacific/chinas-scary-lesson-to-the-world-censoring-the-internet-works/2016/05/23/413afe78-fff3-11e5-8bb1-f124a43f84dc_story.html (дата обращения: 07.10.2016).

лодёжную группу под названием «Корни Надежды»[12]. Активизировались и крупные коммерческие компании. Например, Google выпустил свои версии браузера Chrome и бесплатные версии Google Play и Analytics in Cuba[13]. Вместе с тем, отсутствие свободного доступа в интернет на Кубе является основным сдерживающим фактором. Именно поэтому Google предложил устанавливать точки доступа wi-fi по всей стране. Второй секретарь кубинской коммунистической партии Хосе Рамон Мачадо Вентура на предложение Google ответил: «Нам нужен интернет, но в нашем случае империалисты будут его использовать, чтобы уничтожить Революцию»[14]. Путь Китая и Кубы представляется малоэффективным. В современном мире создание искусственных барьеров для распространения информации негативным образом отражается на развитии страны.

В странах западной Европы на протяжении многих лет проблема информационного суверенитета не являлась первостепенной, поскольку суверенитет в определённой степени защищался национальным законодательством. Например, существовали правовые нормы, требующие регистрации мест сохранения данных в Швеция, в ФРГ обработка данных, касающихся государства, должно было осуществлять само государство, которому они принадлежат и т.д. [3, с. 101]. Однако случай, связанный с электронной слежкой сотрудниками АНБ за политическими партнёрами США в Европе, может дать новый импульс европейской дискуссии о проблеме «информационного суверенитета»[15], основу которого составляет «цифровой суверенитет».

Наиболее актуальным для Российской Федерации представляется технический аспект проблемы. Нашей стране необходима прежде всего независимость в области цифровых технологий. В этой связи следует выделить наиболее важные *компоненты цифрового суверенитета, технически обеспечивающие национальную безопасность*: поисковая система, социальные сети, операционная система и программное обеспечение, микроэлектроника, сетевое оборудование, национальный сегмент сети Интернет, платёжная система, собственные средства защиты, криптографические алгоритмы и протоколы, навигационная система.

Российский сегмент сети Интернет является одним из крупнейших в мире. В доменах «.ru» и «.рф» зарегистрировано более 6 млн адресов; в стране насчитывается более тысячи операторов связи. «Россия занимает третье место в мире по устойчивости национального сегмента интернета к возможным сбоям — более надежными оказались лишь сети Великобритании и США»[16]. Российская Федерация принимает активное участие в глобальном управлении сетью, являясь постоянным участником Internet Governance Forum (IGF)[17].

Создание собственных поисковых систем началось в России в 80-е – начале 90-х гг. В настоящее время в российском сегменте интернета наиболее популярными отечественными системами поиска являются: Rambler, Yandex, Mail.ru.

Rambler – одна из первых российских поисковых систем, разработка которой началась еще в 1991 г. 8 октября 1996 г. поисковая система была запущена. Многие российские пользователи именно с этого момента отсчитывают историю российского сегмента сети Интернет, часто называемого «Рунет». Несмотря на достаточно успешное развитие поисковой системы в начале 2000-х, в 2011 г. компания отказалась от собственного поиска в пользу поисковой системы «Яндекс»[18], которая впервые была анонсирована в Москве 23 сентября 1997 г. На сегодняшний день «Яндекс» остался единственной конкурентоспособной поисковой системой «Рунета», которая по популярности у российских пользователей сравнялась с мировым лидером - Google (график №1). Важным представляется вопрос о юридической принадлежности компании «Яндекс», которая зарегистрирована в России, а весь её уставной капитал принадлежит акционерному обществу Yandex N.V. Регистрацию в Нидерландах пресслужба компании объясняет «исключительно особенностями корпоративного права, а не целью оптимизации налогообложе-

[12] US secretly created «Cuban Twitter» to stir unrest and undermine government // The Guardian. 3 April 2014. [Электронный ресурс]. URL: http://www.theguardian.com/world/2014/apr/03/us-cuban-twitter-zunzuneo-stir-unrest (дата обращения: 07.10.2016).

[13] King B. Google Brings Free Play Store Apps To Cuba For The Few People Who Can Use Them // Android Police.26 November 2014. [Электронный ресурс]. URL: http://www.androidpolice.com/2014/11/26/google-brings-free-play-store-apps-cuba-people-can-use/ (дата обращения: 07.10.2016).

[14] Ravsberg F. Cuban Communist Party Tells Google No Thanks on Free WiFi // Havana Times. 13 July 2015. URL: http://www.havanatimes.org/?p=112542 (дата обращения: 07.10.2016).

[15] Скандал со сбором данных спецслужбами США // РИА Новости. [Электронный ресурс]. URL: http://ria.ru/trend/usa_internet_07062013/ (дата обращения: 07.10.2016).

[16] Коломыченко М. Рунет не уложить // Газета «Коммерсантъ». 07.06.2016. [Электронный ресурс]. URL: http://www.kommersant.ru/doc/3006949 (дата обращения: 07.10.2016).

[17] Internet Governance Forum. [Электронный ресурс]. URL: http://www.intgovforum.org (дата обращения: 07.10.2016).

[18] «Рамблер» отказался от собственного поиска // Радиостанция «Вести ФМ». 24.06.2011. [Электронный ресурс]. URL: http://radiovesti.ru/episode/show/episode_id/10977 (дата обращения: 07.10.2016).

ния»[19]. В 2009 г. компания передала Сбербанку так называемую «золотую акцию» (она позволяет банку блокировать продажу более чем 25% компании). Российские пользователи обслуживаются в российских дата-центрах «Яндекс», а западные серверы компании используются исключительно для индексации зарубежного веба[20]. Несмотря на то, что «Яндекс» является «национальной поисковой системой»[21], в контексте проблемы «цифрового суверенитета» вопрос остается открытым.

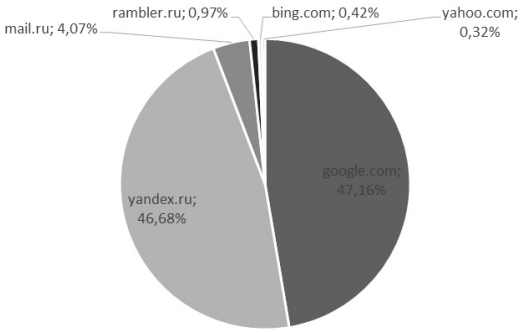

Рис. 1
Figure 1.
Популярность поисковых систем в рунете[22]
Popularity of the search engine in runet

Проблема социальных сетей, по мнению многих аналитиков, тесно связана с национальной безопасностью и суверенитетом [2]. Уже ни для кого не секрет, что социальные сети стали инструментом для проведения так называемых «цветных революций» [12]. Социальные сети — это одновременно и «организационное оружие» и — бизнес-продукт. Крупнейшей социальной сетью на данный момент является Facebook [15], в котором зарегистрировано более 1.4 млрд пользователей. Для российских соцсетей «ВКотнтакте» и «Одноклассники», учитывая, что большая часть пользователей — это наши граждане, подобный показатель представляется недостижимым. Вместе с тем, ещё в 2014 г. «ВКонтакте» вошла в топ-10 крупнейших социальных сетей мира, обогнав такие популярны сервисы, как Instagram, Pinterest и Foursquare. Социальная сеть «ВКонтакте» принадлежит российской компании Mail.Ru Group. Среди активов компании также социальная сеть «Одноклассники», службы мгновенного обмена сообщениями ICQ и «Агент Mail.Ru», служба электронной почты «Почта Mail.Ru», портал и поисковая система Mail.ru и др. сервисы.

Популярность и формальная принадлежность социальной сети России не являются гарантами безопасности [8]. Достаточно ввести несколько поисковых запросов в социальных сетях «Одноклассники» и «ВКонтакте», чтобы обнаружить страницы, содержащие скрытую пропаганду экстремистских идей, информацию, направленную на разжигание межэтнической, межконфессиональной, межсоциальной и межгендерной розни. Существуют также группы, пропагандирующие свержение государственного строя и изменение политической системы [14]. Разумеется, правоохранительные органы и Роскомнадзор работают с отечественными социальными сетями. По требованию Роскомнадзора блокируются сообщества, нарушающие законодательство. По запросу правоохранительных органов социальные сети представляют личные данные пользователя (обычно, необходим именно ip-адрес). По решению суда правоохранительные органы имеют возможность получить доступ и к личной переписке пользователя. В некоторых случаях, согласно внутренним правилам, администрация социальных сетей сама блокирует запрещённый контент. Стоит отметить, что, например, «Правила пользования сайтом ВКонтакте»[23] или «Лицензионное соглашение» сайта «Одноклассники»[24] описывают практически все возможные нарушения законодательства, что теоретически позволят администрации сайта самостоятельно блокировать любой опасный или нежелательный контент. Постепенно социальные сети становятся важным элементом национальной безопасности. Документы, которые были раскрыты Сноуденом и Ассанджем, полностью подтвердили мнение экспертов, что социальные сети разрабатывались в США для осуществления контроля над населением планеты.

Еще в 1947 г. легендарный аналитик ЦРУ Шерман Кент, основоположник «аналитической разведки», считал, что в мирное время до 80% информации можно получать из открытых ис-

[19] Голицына А. «Яндекс» прокомментировал заявления Путина. // «Ведомости». 24.04.2014. [Электронный ресурс]. URL: http://www.vedomosti.ru/technology/articles/2014/04/24/yandeks (дата обращения: 07.10.2016).

[20] «Яндекс» заявил, что не использует для обслуживания россиян зарубежные серверы // ТАСС информационное агентство. 24.04.2014. [Электронный ресурс]. URL: http://tass.ru/ekonomika/1145507 (дата обращения: 07.10.2016).

[21] Путин обнаружил вмешательство Запада в развитие «Яндекса» // INTERFAX.RU. 24.04.2014. [Электронный ресурс]. URL: http://www.interfax.ru/russia/373662 (дата обращения: 07.10.2016).

[22] HotLog за июль 2016 г. [Электронный ресурс]. URL: http://hotlog.ru/global/se?month=3 (дата обращения: 07.10.2016).

[23] Правила пользования сайтом ВКонтакте // ВКонтакте. [Электронный ресурс]. URL: https://new.vk.com/terms (дата обращения: 07.10.2016).

[24] Об утверждении государственной программы Российской Федерации «Развитие электронной и радиоэлектронной промышленности на 2013 - 2025 гг.» // Сайт Правительства РФ. . [Электронный ресурс] URL: http://government.ru/docs/3345/ (дата обращения: 07.10.2016).

точников. Позднее, генерал-лейтенант Самуэль Уилсон заявил, что «90% необходимой информации разведка получает из открытых источников, а остальные 10% добывает агентура» [21, p. 78]. С развитием социальных сетей процент получаемой из открытых источников возрос ещё больше.

Сдерживающим фактором, как это было сказано применительно к Кубе и Китаю, является отсутствие свободного доступ к сети Интернет. С 2013 г. компания Facebook при поддержке компаний Samsung, Ericsson, MediaTek, Opera Software, Nokia и Qualcomm начала развивать проект Internet.org[25]. Суть данной инициативы состояла в предоставлении бесплатного доступа к ряду интернет-ресурсов жителям наименее развитых стран. Список доступных ресурсов до апреля 2015 г. был строго ограничен и определялся самой компанией Facebook. Обращает внимание тот факт, что среди доступных ресурсов и в настоявшее время нет правительственных сайтов, учебных заведений; отсутствуют многие популярные развлекательные сайты. Таким образом, как справедливо отмечает обозреватель журнала PCWorld Майк Элган, «Facebook получает клиентов, данные пользователей и возможность монетизации благодаря рекламе, в то время как люди ограждаются от полноценного интернета и от конкурирующих компаний и других услуг, которые могли бы отвлечь их от того, чтобы проводить большую часть своего времени на Facebook»[26].

Согласно документам, опубликованным Сноуденом, разведка активно использует данные, полученные из социальных сетей. Так, более 24%[27] процентов ресурсов глобальной системы радиоэлектронной разведки «Эшелон» [20] отведено именно под мониторинг социальных сетей.

Проект «Эшелон» был разработан и координируется АНБ. Основная цель проекта состоит в перехвате электронной корреспонденции, факса, телекса и телефонной связи во всех телекоммуникационных сетях. Объектами наблюдения являются невоенные цели, такие как правительства, организации, предприятия и физические лица. Система, используя сложный программно-аппаратный комплекс, перехватывает и анализирует данные для идентификации и извлечения полезной информации. «Эшелон» анализирует огромный массив перехваченной информации на предмет наличия ключевых слов (имена, места, субъекты, персональные данные физических лиц).

Одними из основных инструментов перехвата информации «Эшелона» являются также и вполне легальные программные средства крупных американских ИТ-корпораций, например, Microsoft - ОС Windows, продукты Google.

В ответ на разработку системы «Эшелон» в 1970-х гг. был создан отечественный аналог – «Система объединённого учёта данных о противнике» (СОУД). Соглашение о создании данной системы было подписано странами Варшавского договора в 1977 г., а сама система запущена в 1979 г. Официальной целью являлось предотвращение террористических актов в СССР во время Олимпиады 1980 г. в Москве. Система была переоснащена и доработана в 2000-х гг. Однако в силу секретности данные о её текущем состоянии нам не известны.

Большинство компьютеров в нашей стране оснащено продукцией компаний Microsoft или Apple. Данное обстоятельство ставит Россию в прямую зависимость от западных корпораций. Например, в случае введения санкций в виде запрета на продажу операционной системы (ОС), экономика нашей страны может сильно пострадать. Ещё одну опасность таит использование иностранной закрытой коммерческой операционной системы. Готовую ОС достаточно сложно проанализировать на наличие скрытых уязвимостей, которые могут представлять определённую угрозу информационной безопасности РФ. Корпорация никогда не предоставит полный исходный код собственной продукции, поскольку данная информация составляет коммерческую тайну, интеллектуальную собственность. Покупая продукцию западных корпораций (например, Windows и Microsoft Office), Россия не только лишает себя возможности достижения суверенитета в информационном пространстве, но и прямо вкладывает средства в экономику другой страны.

Для обеспечения информационной безопасности и цифрового суверенитета России важным является создание отечественной операционной системы и программного обеспечения. Данный процесс – явление сложное и многофакторное, которое основывается на достижениях мировой научной мыли и разработках предыдущих лет.

Упомянутые выше компании Microsoft и Apple начали разработку собственных операционных систем с покупки уже существующих, используя их в качестве основы. Так, компания Microsoft свою первую операционную систему Xenix создавала на базе ОС Version 7 Unix от компании AT&T [13, с. 787]. Наиболее известной операционной системой компании Microsoft стала MS-DOS, основанная на 86-DOS от Seattle

[25] Объединить весь мир // Internet.org. [Электронный ресурс]. URL: https://info.internet.org/ru/?noredirect=ru_RU (дата обращения: 07.10.2016).

[26] Elgan M. The surprising truth about Facebook's Internet.org // PCWorld. 15 February 2016. [Электронный ресурс]. URL: http://www.pcworld.com/article/3033274/internet/the-surprising-truth-about-facebooks-internetorg.html (дата обращения: 07.10.2016).

[27] Тихонов С. Как «ВКонтакте» и «Одноклассники» отстояли независимость России // Эксперт Online. [Электронный ресурс]. URL: http://expert.ru/2013/11/20/kak-vkontakte-i-odnoklassniki-otstoyali-nezavisimost-rossii/ (дата обращения: 07.10.2016).

Computer Products[28]. Компании потратили несколько десятков лет, чтобы получить программный продукт в том виде, в котором мы привыкли его видеть в настоящее время.

Стоит отметить тот факт, что отдельные компании и коллективы делали и делают попытки создания абсолютно новых операционных систем. Например, MenuetOS[29] была разработана группой любителей-энтузиастов, основной дистрибутив которой умещается на дискету (1,44 Мб). Несмотря на небольшой размер это полноценная операционная система, которая имеет определённый набор драйверов, браузер, текстовый процессор, графический редактор и т.д. В MenuetOS встроена полная поддержка файловых систем FAT12/16/32, а для чтения доступны NTFS, ISO 9660, Ext2/3/4. ОС представляет собой скорее интересный эксперимент любителей, чем продукт пригодный для реального использования.

Операционная система под названием «Реакт ОС» (ReactOS) создавалась в России также энтузиастами-любителями, которые ставили своей целью сделать ОС полностью совместимую с Windows. Проект до сих пор не завершён, но уже начал морально устаревать[30]. Разработчики рассчитывали, что толчком к распространяю ОС станет прекращение расширенной поддержки Windows XP в апреле 2014 г., однако этого не случилось. Сложно не согласиться с мнением генерального директора компании Alt Linux А. Новодворского, что ReactOS пока не показывает результатов, которые могли бы быть применимы в реальной практике заказчиков. Число Windows-приложений и драйверов, работающих под ReactOS, недостаточно велико»[31].

В сложившейся ситуации с разработкой российской операционной системы выходом могло бы стать использование так называемого открытого программного обеспечение (англ. open-source software), т.е. с открытым исходным кодом, который доступен для просмотра, изучения и изменения. В зависимости от лицензионного соглашения, возможно или прямо заимствовать исходный код, или изучать использованные алгоритмы и технологии, а затем внедрять их в собственное программное обеспечение. Таким образом, возможно, например, создать отечественную операционную систему, взяв за основу ядро Linux.

Илья Массух, будучи заместителем министра связи, ещё в 2010 г. сообщил о ведущихся работах по созданию национальной операционной системы к 2020 г. Федеральный ядерный центр в Сарове (РФЯЦ-ВНИИЭФ) на основе ядра Linux ведёт разработку отечественной ОС под названием «Синергия». В 2014 г. над данным проектом работало более 70 сотрудников ядерного центра и к 2015 г. разработка перешла в стадию тестирования продукта. ОС «Синергия», по мнению разработчиков, позволит в перспективе отказаться от ОС Windows.

ОС «Синергия» является 64-битной операционной системой с мандатным принципом контроля доступа и разделением ресурсов. В ОС интегрирован гипервизор первого уровня с мультидоменной структурой ввода-вывода для виртуализации, а также СУБД на базе PostgreSQL, которая должна заменить СУБД Oracle. По информации опубликованной в T-adviser, «платформа на базе ОС ‘Синергия’ сможет одновременно работать в трёх сетях с информацией различной степени конфиденциальности (гостайна, ДСП, интернет) по технологии ‘тонкого клиента’, включая работу с инженерными приложениями CAD, CAM, CAE»[32].

Компанией АО МЦСТ (первоначально «Московский центр SPARC-технологий») для вычислительного комплекса с архитектурой SPARC и «Эльбрус» создала операционную систему ОС «Эльбрус». Данная система (как и ОС «Синергия») основана на базе ядра Linux (текущая версия на Linux 2.6.33). ОС «Эльбрус» является многозадачной операционной системой с многопользовательским режимом. «Для неё разработаны особые механизмы управления процессами, виртуальной памятью, прерываниями, сигналами, синхронизацией, поддержка тегированными вычислениями»[33].

Для использования вычислительного комплекса серии «Эльбрус» в ряде ответственных систем проделана фундаментальная работа по преобразованию ОС Linux в операционную систему, поддерживающую режим работы в реальном времени, для чего были реализованы актуальные оптимизации АО МЦСТ.

[28] Shustek L. Software Gems: The Computer History Museum Historical Source Code Series // Computer History Museum. [Электронный ресурс]. URL: http://www.computerhistory.org/atchm/microsoft-ms-dos-early-source-code/ (дата обращения: 07.10.2016).

[29] MenuetOS. [Электронный ресурс]. URL: http://menuetos.net/ (дата обращения: 07.10.2016).

[30] ReactOS. [Электронный ресурс]. URL: http://www.reactos.org/ (дата обращения: 07.10.2016).

[31] Легезо Д. Школьник попросил Медведева выделить 1 млн евро на разработку «бесплатной Windows» // CNews. 01.09.2011. [Электронный ресурс]. URL: http://www.cnews.ru/news/top/shkolnik_poprosil_medvedeva_vydelit (дата обращения: 07.10.2016).

[32] Синергия Операционная система. // TAdviser. [Электронный ресурс]. URL: http://www.tadviser.ru/index.php/%D0%9F%D1%80%D0%BE%D0%B4%D1%83%D0%BA%D1%82:%D0%A1%D0%B8%D0%BD%D0%B5%D1%80%D0%B3%D0%B8%D1%8F_%D0%9E%D0%BF%D0%B5%D1%80%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D0%B0%D1%8F_%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%B0 (дата обращения: 07.10.2016).

[33] Операционная система Эльбрус // АО «МЦСТ». [Электронный ресурс]. URL: http://www.mcst.ru/os_elbrus (дата обращения: 07.10.2016).

Кроме указанных выше операционных систем, разработка которых ещё не завершена, существуют специализированные дистрибутивы Linux с повышенным уровнем защищенности. Ещё на этапе проектирования в них были учтены повышенные требования к защищённости, которые предъявляются к компьютерным системам управления критически важными объектами [9, с. 168-216]. Среди подобных дистрибутивов, разрабатываемых и совершенствуемых в десятках активно развивающихся проектов, в качестве примера следует привести продукцию компаний НТЦ ИТ РОСА и ОАО НПО РусБИТех. Первая разработала семейство операционных систем ROSA Linux, основанных на Mandriva (десктопный вариант) и RedHat (серверный вариант). Дистрибутивы ROSA Linux сертифицированы ФСТЭК России и российским Министерством обороны для обработки конфиденциальной информации и персональных данных, а также обработки сведений, составляющих государственную тайну. Например, ОС РОСА DX «Никель» 1.0, согласно информации, опубликованной на официальном сайте компании, «сертифицирована (до весны 2017 г.) Восьмым управлением ГШ ВС РФ, со встроенными средствами защиты от несанкционированного доступа к информации — на соответствие РД СВТ по 4 классу и РД НДВ по 3 уровню контроля»[34]. Вторая компания — научно-производственное объединение «Русские базовые информационные технологии» (РусБИТех) — совместно со специалистами Академии ФСБ разработала операционную систему специального назначения Astra Linux Special Editon» (ОС Astra Linux)[35]. Дистрибутив сертифицирован в системах сертификации средств защиты информации ФСБ России, ФСТЭК России и Минобороны России. ОС Astra Linux обеспечивает защиту информации содержащую сведения, составляющие государственную тайну с грифом не выше «совершенно секретно».

Ещё одним важным компонентом информационного суверенитета, является российская микроэлектроника. В 1970-80-х гг. СССР занимал второе место в мире после США по уровню развития микроэлектроники. В 1990-е гг. российская экономика находилась в кризисе, электронная промышленность пришла в упадок [11]. В августе 2007 г. была принята «Стратегия развития электронной промышленности РФ до 2025 г.»[36]. В данном документе констатируется тяжёлое состояние российской электронной промышленности и подчёркивается, что страна не только отстала от ведущих держав, но и утратила часть собственного потенциала после распада СССР; доля России на мировом рынке электронной компонентной базы снизилась до 0,23%. Даже внутри страны доля импортной электронной компонентной базы составила 60% от общего объёма электронных изделий. В 2008 г. была запущена программа «Развитие электронной компонентной базы и радиоэлектроники» на 2008-2015 гг.[37].

Указанные программы стали составной частью новой государственной программы Российской Федерации «Развитие электронной и радиоэлектронной промышленности на 2013-2025 гг.», утверждённой 15 декабря 2012 г. «Целью программы является повышение конкурентоспособности радиоэлектронной промышленности посредством создания инфраструктуры для развития приоритетных направлений, интеграции в международный рынок и реализации инновационного потенциала»[38]. На её реализацию предусмотрено выделить из федерального бюджета 65743 млн руб. и 37198 млн руб. из внебюджетных источников[39].

29 сентября 2015 г. на совещании по вопросу развития рынка микроэлектроники В.В. Путин отметил, что «с 2009 г. отечественный рынок микроэлектроники вырос почти в три раза – до 150 млрд рублей, а объём экспорта гражданской продукции увеличился примерно в два раза»[40]. В своём выступлении президент РФ подчеркнул значимость развития отрасли для национальной безопасности страны и отметил существующую опасность срыва поставок импортного оборудования. Геополитическое противостояние вынуждает Россию быстрыми темпами двигаться по пути импортозамещения, уделяя пристальное внимание развитию элементной базы в сфере

[34] ООО «НТЦ ИТ РОСА». [Электронный ресурс]. URL: https://www.rosalinux.ru/products/ (дата обращения: 07.10.2016).

[35] Astra Linux. [Электронный ресурс]. URL: http://www.astra-linux.com/products/alse.html (дата обращения: 07.10.2016).

[36] Об утверждении Стратегии развития электронной промышленности России на период до 2025 года // «Техэксперт». [Электронный ресурс]. URL: http://docs.cntd.ru/document/902063681 (дата обращения: 07.10.2016).

[37] Федеральная целевая программа «Развитие электронной компонентной базы и радиоэлектроники» на 2008 - 2015 гг. // Департамент государственных целевых программ и капитальных вложений Минэкономразвития России. [Электронный ресурс]. URL: http://fcp.economy.gov.ru/cgi-bin/cis/fcp.cgi/Fcp/ViewFcp/View/2015/246 (дата обращения: 07.10.2016).

[38] Федеральная целевая программа «Развитие электронной и радиоэлектронной промышленности на 2013 - 2025 гг.» // Департамент государственных целевых программ и капитальных вложений Минэкономразвития России. [Электронный ресурс]. URL: http://fcp.economy.gov.ru/cgi-bin/cis/fcp.cgi/Fcp/ViewGP/View/2014/19/ (дата обращения: 07.10.2016).

[39] Там же.

[40] Совещание по развитию микроэлектроники // Администрация Президента России. 29.09.2015. [Электронный ресурс]. URL: http://kremlin.ru/events/president/news/50397 (дата обращения: 07.10.2016).

телекоммуникаций, транспорта, электронных документов, а также в финансовом секторе.

Можно наблюдать первые результаты политики импортозамещения в области микроэлектроники. В России на отечественных чипах стал возможен выпуск смарт-карт, электронных удостоверений, паспортов и других электронных документов. Например, Московский метрополитен ежегодно получает более 235 млн билетов, Мосгортранс - 80 млн билетов. Постепенно вводятся в эксплуатацию электронные билеты и в регионах РФ. Отечественные чипы используются в банковской сфере, в том числе в процессе создания национальной платежной системы.

В свете развития одного из основных элементов информационного суверенитета – микроэлектроники, сложно переоценить важность создания современного российского процессора. В настоящее время на микропроцессорном рынке господствуют две американские компании: Intel и AMD. Подавляющее большинство серверных и настольных компьютеров основано именно на их процессорах. Данное обстоятельство не только ставит Россию в зависимость от продукции американских корпораций, но и таит скрытую опасность. Ещё в 2005 г. Научный совет министерства обороны США опубликовал отчёт[41], в котором была отмечена опасность производства процессоров за пределами США. В документе подчёркивалось, что существует возможность намеренного изменения процессора в ходе проектирования или производства, что может поставить под угрозу национальную безопасность. Данная угроза некоторое время считалась гипотетической, но в 2013 г. её реальность, опытным путем доказали: Георг Беккер, Франческо Регаццони, Кристоф Паар и Уэйн Берлесон. Эта интернациональная команда учёных, возглавляемая профессором из университета штата Массачусетс Г. Беккером, смогла создать две версии «трояна аппаратного уровня» [16], которые не обнаруживались традиционными средствами. Таким образом, стало окончательно ясно, что внедрённый в процессор «троянский конь» или «аппаратная закладка» могут оставаться незамеченными, угрожая не только информационной безопасности, но и на фундаментальном уровне подрывая обороноспособность страны.

Первые советские микропроцессоры появились в 1970-е гг. В 1977 г. была выпущена серия К580, клон Intel i8080, а с 1980-х гг., в условиях политики «перестройки», социально-экономической нестабильности, СССР фактически полностью перешёл к копированию западных. Это сильно затормозило развитие российской микроэлектроники. Однако, разработка микропроцессоров продолжалась в отдельных НИИ. В настоящее время можно говорить о создании как минимум трёх перспективных отечественных процессоров: «Эльбрус 8С» (компания МЦСТ), Baikal (компания «Т-Платформы») и «Мультиклет R1». Создание каждого из них стало значимым событием в развитии российской микроэлектроники, которое вызвало дискуссию на страницах СМИ, в российском сегменте сети Интернет. Дискуссия разгорелась вокруг таких вопросов, как экономическая конкурентоспособность данной продукций, производительность процессоров, их значение в рамках политики импортозамещения.

В связи с тем, что данные вопросы непосредственно связаны с национальной безопасностью, стоит попытаться более подробно их проанализировать. Разработка любого процессора начинается с выбора его архитектуры, определяющей устройство, набор исполнительных команд. Не вдаваясь в тонкости определения понятия процессорной архитектуры, следует отметить, что именно она во многом определяет назначение процессора и его потенциал. Наиболее распространенными являются: архитектура x86 (от англ. Intel 80x86), а также архитектуры разработанные в соответствии с концепцией RISC (от англ. restricted (reduced) instruction set computer - сокращённым набором команд) или, иными словами, RISC-подобные, как ARM (от англ. Advanced RISC Machine - усовершенствованная RISC-машина) и MIPS (от англ. Microprocessor without Interlocked Pipeline Stages).

Большая часть процессоров для настольных компьютеров и серверов имеет x86(x86-64) архитектуру. Под x86 написано колоссальное количество программного обеспечения, достигнута рекордная производительность. Вместе с тем, данная архитектура считается малоперспективной для использования в мобильных устройствах в связи с большим энергопотреблением. Эту архитектуру невозможно лицензировать. Как уже было отмечено, СССР копировал процессоры, созданные по данной архитектуре. В настоящее время подобное нарушение авторского права стало бы как минимум экономически невыгодным, не говоря уже о стратегической нецелесообразности, препятствием на пути достижения информационного суверенитета.

Таким образом, возможно или использовать собственную архитектуру, что потребует создание всего комплекса программного обеспечения, или разрабатывать процессоры на основе лицензируемой, например, на MIPS. Первый вариант был избран при создании процессоров «Эльбрус 8С» (компания МЦСТ) и «Мультиклет R1», второй - для Baikal (компания Т-Платформы). Разработка микропроцессоров «Эльбрус» началась ещё в 1970-е гг.: был создан 10-процессорный комплекс на базе TTL логики. В 1985 г. вышла его усовершенствованная версия. В 1990-е гг. в сложных экономических условиях разработка и производство микропроцессоров продолжа-

[41] U.S. Department of Defense. Defense science board task force on high performance microchip supply. February 2005. [Электронный ресурс]. URL: http://www.acq.osd.mil/dsb/reports/ADA435563.pdf (дата обращения: 07.10.2016).

лась на основе открытой архитектуры SPARC, созданной Sun Microsystems.

Улучшение экономической ситуации в 2000-е гг., курс на импортозамещение, а также накопленные к тому времени компанией МЦСТ разработки, позволили в 2008 г. перейти к производству принципиально нового российского микропроцессора на VLIW архитектуре. Данный микропроцессор, в первую очередь, предполагалось использовать в системах ПВО и ПРО. В 2014 г. начался серийный выпуск микропроцессора «Эльбрус-4С», изготовленного по технологии 65 нм. Процессор содержит 4 ядра, которые функционируют на частоте 800 МГц. Каждое из них оснащено 2 МБ кэш-памяти. В 2015 г. была изготовлена и передана органам исполнительной власти первая партия серверов на базе данного микропроцессора. По информации, опубликованной на официальном сайте Объединённой приборостроительной корпорации, в 2016 г. начата разработка вычислительной техники на базе нового российского 8-ядерного микропроцессора «Эльбрус-8С»[42].

Стоит отметить, что некоторые аналитики выражают скептицизм относительно перспектив российских микропроцессоров данной серии. Например, обозреватель журнала PC World Марк Хахман в статье, озаглавленной «С российским процессором Эльбрус, ПК был бы фантастическим в 1999 г.»[43], отмечает, что микропроцессоры «Эльбрус» не могут конкурировать с продукцией Intel в связи с низким техпроцессом и производительностью. Сложно согласиться с мнением автора статьи. Микропроцессор «Эльбрус-4С», о котором речь идёт в публикации, не совсем корректно сравнить с продукцией корпорации Intel, поскольку он был выпущен в первую очередь с целью создания «техники для государства и стратегических секторов, где остро стоит вопрос защиты информации и ухода от небезопасных технологий»[44]. Стратегическое назначение микропроцессора может несколько снизить значимость показателей производительности, а также подразумевать оптимизацию микропроцессора и программного обеспечения под специфические задачи. Справедливости ради стоит обратить внимание, что на официальном сайте компании МЦСТ указаны достаточно высокие показатели производительности, например, для «Эльбрус-4С» - 25 Gflops (64 разряда, двойная точность), а для «Эльбрус-8С» 125 Gflops (64 разряда, двойная точность). В связи с закрытостью компании МЦСТ нет достоверной информации о том, каким образом данные были получены: указана ли теоретическая производительность или согласно синтетическим тестам, включают ли эти цифры производительность DSP процессора и т.д. Острой критике в СМИ подвергается выбор VLIW архитектуры микропроцессора. Не вдаваясь в технические подробности и не пытаясь сравнить различные архитектуры, отметим, что Россия не стала первой страной, выпустившей микропроцессоры с VLIW архитектурой. Корпорация Intel совместно с Hewlett Packard разработала IA-64 (Intel Architecture-64) архитектуру, основанную на VLIW. В 2001 г. Intel выпустила первый IA-64 процессор линейки Itanium. Процессоры Itanium продолжают выпускаться, однако их сложно назвать коммерчески успешным продуктом. С другой стороны, если рассматривать процессоры «Эльбрус» исключительно с точки зрения национальной безопасности, достижения цифрового суверенитета, то коммерческая составляющая отходит на второй план.

Что касается упомянутого выше процессора Baikal, то он ориентирован на динамично развивающийся рынок коммуникационных решений и встроенных систем. Процессор «Мультиклет R1» может быть востребован в приборостроительной отрасли, оборонной и авиакосмической промышленности, научно-исследовательских и образовательных центрах.

Стоит отметить, что микропроцессор является основным, но не единственным компонентом компьютера. В настоящее время, например, нет достоверной информации о выпуске отечественных жестких дисков и графических процессоров.

Подъём российской микроэлектроники способствовал развитию сетевого и телекоммуникационного оборудования. Продукция нескольких десятков отечественных компаний уже сумела хорошо зарекомендовать себя на российском рынке, что безусловно способствует достижению информационного суверенитета.

Достижение цифрового суверенитета невозможно без создания шифровальных (криптографических) средств защиты информации, обеспечивающих безопасное хранение и передачу данных. Приказом ФСБ России от 9 февраля 2005 г. № 66 было утверждено «Положение о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации»[45]. С целью практической реализации данного положения, при-

[42] ОПК разрабатывает защищенное оборудование на базе «Эльбруса-8С» // Госкорпорация Ростех. 20.01.2016. [Электронный ресурс]. URL: http://rostec.ru/news/4517650 (дата обращения: 07.10.2016).

[43] Hachman M. Russia's homegrown Elbrus processor and PC would be fantastic in 1999 // PC World. 12 May 2015. [Электронный ресурс]. URL: http://www.pcworld.com/article/2920988/russias-homegrown-elbrus-processor-and-pc-would-be-fantastic-in-1999.html (дата обращения: 07.10.2016).

[44] ОПК разрабатывает защищенное оборудование на базе «Эльбруса-8С» // Госкорпорация Ростех. 20.01.2016. [Электронный ресурс]. URL: http://rostec.ru/news/4517650 (дата обращения: 07.10.2016).

[45] Приказ ФСБ РФ от 9 февраля 2005 г. N 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)» (с изменениями и дополнениями) // Портал ГАРАНТ.РУ. [Электронный ресурс]. URL: http://base.garant.ru/187947/ (дата обращения: 07.10.2017).

казом Ростехрегулирования от 28 декабря 2007 г. был создан технический комитет по стандартизации «Криптографическая защита информации» (ТК 26). С 2010 по 2015 гг. ТК26 проводил комплексную работу по обновлению национальных стандартов криптографии. 7 августа 2012 г. Федеральное агентство по техническому регулированию и метрологии утвердила ГОСТ Р 34.10–2012 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи»[46] и ГОСТ Р 34.11–2012 «Информационная технология. Криптографическая защита информации. Функция хеширования»[47]. 19 июня 2015 г. приказами Федерального агентства по техническому регулированию и метрологии № 749-ст и 750-ст национальных стандартов ГОСТ Р 34.12–2015[48] и ГОСТ Р 34.13–2015[49] были окончательно определены алгоритмы блочного шифрования и режимы их работы.

Перспективы применения российских алгоритмов шифрования обсуждаются многими экспертами. Российские алгоритмы обладают высокой стойкостью к взлому, а их программная реализация (без использования специальных конструкций SSE/AVX) позволяет добиться сопоставимой с западными аналогами скорости шифрования\дешифровки [6]. Вместе с тем, в настоящее время можно констатировать отсутствие аппаратной поддержки российских алгоритмов шифрования как в западных, так и в отечественных микропроцессорах. Стоит отметить, что наличие в последних поколениях микропроцессоров Intel и AMD расширения системы команд AES (Advanced Encryption Standard) даёт значительное ускорение приложений, использующих шифрование по алгоритму AES [17]. Учитывая, что российские процессоры имеют архитектуру с сокращённым набором команд, перспективы использования отечественных алгоритмов представляются не столь радужными. Успешная реализация алгоритмов ГОСТ 28147–89 и ГОСТ Р 34.12-2015 на графическом процессоре (Graphics Processing Unit, GPU), которая подчёркивается некоторыми экспертами [7], представляется слабым доводом в пользу отечественных алгоритмов шифрования, поскольку, как было отмечено выше, графические процессоры в России пока не производятся.

С криптографическим проблемами связан ещё один аспект национальной безопасности – борьба с терроризмом. В июле 2016 г. были приняты два законопроекта, фигурирующие в СМИ под названием «Пакет Яровой» (по фамилии одного из его авторов — депутата Государственной думы V и VI созывов Ирины Яровой). Законопроект № 1039149-6 «О внесении изменений в отдельные законодательные акты Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности»[50] обязывает операторов связи до полугода хранить записи телефонных разговоров, SMS и интернет-трафик пользователей, и до трёх лет информацию о самом факте приёма или передачи данных. Поскольку значительная часть информации шифруется, в законопроект были внесены поправки, согласно которым социальные сети, мессенджеры, почтовые сервисы, а также операторы связи должны предоставлять ключи для дешифровки данных по требованию властей. Подобное нововведение технически легко реализуемо по отношению к российским компаниям. Что касается западных сервисов, например, Gmail, то вопрос расшифровки данных остаётся открытым. Справедливости ради отметим, что использование западных сервисов соотечественниками может представлять угрозу национальной безопасности не только в связи со сложностями антитеррористической борьбы. Согласно информации, обнародованной Эдвардом Сноуденом в 2013 г., Агентство национальной безопасности США создало в 2007 г. систему разведки (программу) Prism [18], позволяющую спецслужбам получать прямой доступ к серверам компаний без санкции суда. Таким образом, американские спецслужбы уже имеют прямой доступ к серверам девяти ведущих интернет-компаний: Microsoft (с 2007 года), Yahoo (2008), Google, Facebook, PalTalk

[46] Об утверждении национального стандарта. Приказ Росстандарта от 7 августа 2012 года №215-ст // Техэксперт - электронный фонд правовой и нормативно-технической документации. [Электронный ресурс]. URL: http://docs.cntd.ru/document/902368267 (дата обращения: 07.10.2016).

[47] Голицына А. «Яндекс» прокомментировал заявления Путина // «Ведомости». 24.04.2014. [Электронный ресурс]. URL: http://www.vedomosti.ru/technology/articles/2014/04/24/yandeks (дата обращения: 07.10.2016).

[48] ГОСТ Р 34.12-2015. Информационная технология. Криптографическая защита информации. Блочные шифры // Российский Архив Государственных Стандартов, а также строительных норм и правил (СНиП) и образцов юридических документов. [Электронный ресурс]. URL: http://www.rags.ru/gosts/gost/60339/ (дата обращения: 07.10.2016).

[49] ГОСТ Р 34.13-2015 Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров // Техэксперт - электронный фонд правовой и нормативно-технической документации. [Электронный ресурс]. URL: http://docs.cntd.ru/document/1200121984 (дата обращения: 07.10.2016).

[50] Законопроект № 1039149-6 «О внесении изменений в отдельные законодательные акты Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности» // Государственная Дума Федерального Собрания Российской Федерации. [Электронный ресурс]. URL: http://asozd2.duma.gov.ru/main.nsf/(Spravka)?OpenAgent&RN=1039149-6 (дата обращения: 07.10.2016).

(все три с 2009 г.), YouTube (2010), AOL, Skype, (обе с 2011 г.) и Apple (2012)[51].

Российские программные средства обеспечения информационной безопасности развиваются достаточно активно. В «Единый реестр российских программ для электронных вычислительных машин и баз данных» входят более 260 программных продуктов[52].

Важным звеном национальной безопасности и цифрового суверенитета является глобальная навигационная система. Первые спутники отечественной «Глобальной навигационной спутниковой системы» (ГЛОНАСС) начали функционировать ещё в 1982 г., а основные работы над её созданием завершились к 1993 г. ГЛОНАСС была официально принята в эксплуатацию Министерством обороны России. Два года спустя система достигла своего штатного состояния в 24 спутника. Вместе с тем, в связи с экономическими проблемами, поддержание работоспособности ГЛОНАСС в 90-е гг. практически не проводилось. Число работающих спутников сократилось к 2001 г. до шести. Систему ГЛОНАСС удалось восстановить благодаря принятой в 2001 г. федеральной целевой программе «Глобальная навигационная система»[53]. К сентябрю 2010 г. количество спутников достигло 26-ти, обеспечено полное покрытие Земли. 7 декабря 2015 г. строительство ГЛОНАСС было официально завершено, систему предъявили заказчику — Министерству обороны РФ[54]. По точности система ГЛОНАСС уже приблизилась к показателям американской системы GPS (Global Positioning System). В рамках федеральной целевой программы «Поддержание, развитие и использование системы ГЛОНАСС на 2012 - 2020 гг.»[55] планируется дальнейшая модернизация отечественной навигационной системы, повышение точности ГЛОНАСС (до 0,6 м).

Идея создания Национальной платёжной системы обсуждалась экспертами ещё в начале 90-х гг., однако, в связи с особенностями внутренней и внешней политики Российской Федерации того периода, практические шаги для её реализации предприняты не были [1]. 85% мировых транзакций по пластиковым картам проводилось двумя международными платёжными системами (МПС) — MasterCard и Visa, а вся информация, включая российскую, обрабатывалась на их терминалах. Безусловно, подобная практика могла стать угрозой национальной безопасности, информационному суверенитету. 27 июня 2011 г. был принят федеральный закон N 161-ФЗ «О национальной платёжной системе»[56]. Закон мало что изменил на практике, поскольку вопрос о создании национальной системы платёжных карт на тот момент в нём не был оговорен.

21 марта 2014 г., в связи с санкциями США, платёжные системы Visa и MasterCard заблокировали пластиковые карточки ряда российских банков. Реальная угроза национальной безопасности России потребовала внесения поправок в Федеральный закон «О национальной платёжной системе», позволяющих создать инфраструктуру для осуществления денежных переводов внутри России, «Национальную систему платежных карт» (НСПК). Таким образом, в 2015 г. удалось полностью перевести на процессинг НСПК все внутрироссийские транзакции Visa и MasterCard. В настоящее время российская национальная платёжная система активно развивается. Она получила официальное название «Мир», были заключены соглашения с MasterCard, Japan Credit Bureau и American Express. Согласно данным, опубликованным в РИА «Новости», «банки РФ уже выпустили 537 тыс. карт национальной платежной системы 'Мир', которые принимают более полумиллиона банкоматов и POS-терминалов»[57].

Проведённый анализ компонентов цифрового суверенитета России позволяет утверждать, что достижение информационного суверените-

[51] Greenwald G., MacAskill E. NSA Prism program taps in to user data of Apple, Google and others // The Guardian. 7 June 2013. [Электронный ресурс]. URL: https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data (дата обращения: 07.10.2016).

[52] Единый реестр российских программ для электронных вычислительных машин и баз данных // Официальный сайт оператора единого реестра российских программ для электронных вычислительных машин и баз данных в информационно-телекоммуникационной сети «Интернет». [Электронный ресурс]. URL: https://reestr.minsvyaz.ru/reestr/ (дата обращения: 07.10.2016).

[53] Федеральная целевая программа «Глобальная навигационная система» // Департамент государственных целевых программ и капитальных вложений Минэкономразвития России. [Электронный ресурс]. URL: http://fcp.economy.gov.ru/cgi-bin/cis/fcp.cgi/Fcp/ViewFcp/View/2006/117 (дата обращения: 07.10.2016).

[54] Чуберко И. Система ГЛОНАСС сдана Минобороны для финальных испытаний // «Газета Известия». 07.12.2015. [Электронный ресурс]. URL: http://izvestia.ru/news/598340 (дата обращения: 07.10.2016).

[55] Федеральная целевая программа «Поддержание, развитие и использование системы ГЛОНАСС на 2012 - 2020 годы» // Департамент государственных целевых программ и капитальных вложений Минэкономразвития России. [Электронный ресурс]. URL: http://fcp.economy.gov.ru/cgi-bin/cis/fcp.cgi/Fcp/ViewFcp/View/2016/396 (дата обращения: 07.10.2016).

[56] Федеральный закон от 27 июня 2011 г. N 161-ФЗ «О национальной платежной системе» (с изменениями и дополнениями) // ЭПС «Система ГАРАНТ». 07.12.2015. [Электронный ресурс]. URL: http://base.garant.ru/12187279/#help (дата обращения: 07.10.2016).

[57] Российские банки выпустили 537 тысяч карт «Мир» // РИА Новости. 09.09.2016. [Электронный ресурс] URL: https://ria.ru/economy/20160909/1476485837.html (дата обращения: 07.10.2016).

та возможно в недалёком будущем. Очередным шагом на пути достижения информационной безопасности стало решение главы администрации президента РФ Сергея Иванова (решением президента от 12 августа 2016 г. руководителем администрации президента РФ назначен А. Э. Вайно) от 3 февраля 2016 г. о создании рабочей группы «по использованию информационно-телекоммуникационной сети Интернет в отечественной экономике при формировании её новой технологической основы и в социальной сфере»[58]. 28 сентября подгруппа «Интернет+суверенитет» рассмотрела проект дорожной карты, основной целью создания которой является «импортозамещение программного обеспечения и оборудования, снижение критической зависимости от зарубежных технологий и промышленной продукции в отрасли информационных технологий и телекоммуникаций»[59]. О важности данной проблемы говорит и тот факт, что правительством подготовлена новая редакция «Доктрины информационной безопасности Российской Федерации», в которой впервые используется понятие «суверенитет в информационной сфере»[60].

Таким образом, основной отличительной особенностью российской технической базы по обеспечению информационного суверенитета является неравномерность и фрагментарность развития её компонентов. Наибольший прогресс достигнут в развитии таких компонентов как российские поисковые системы, социальные сети, национальный сегмент сети Интернет и навигационная система, которая уже способна в полной мере обеспечивать национальную безопасность. Российское программное и аппаратное обеспечение требует ускоренного развития для обеспечения информационного суверенитета, национальной безопасности России. Наибольшее внимание заслуживает российская платёжная система, поскольку данный вопрос находится в прямой зависимости от направления развития экономики страны. Проблема обеспечения информационного суверенитета в значительной степени связана с вопросами принятия государственных решений, приведения нормативной, законодательной базы в соответствие с концепцией национальной безопасности страны.

Сохранение государственного суверенитета, национальной безопасности в значительной степени зависит от информационной безопасности, независимости в области цифровых технологий, цифрового суверенитета. В «Доктрине информационной безопасности Российской Федерации», утверждённой президентом Российской Федерации В.Путиным 9 сентября 2000 г., сказано: «Национальная безопасность Российской Федерации существенным образом зависит от обеспечения информационной безопасности, и в ходе технического прогресса эта зависимость будет возрастать»[61].

Список литературы

1. Ануреев С.В. Платежные системы и их развитие в России. М.: Финансы и статистика, 2011. 288 с.
2. Балуев Д.Г. Влияние современных социальных медиа на информационный суверенитет России: основные подходы к исследованию // Государственное и муниципальное управление. Ученые записки СКАГС. № 3. 2015. С. 140-143.
3. Батурин Ю.М., Жодзижский А.М. Компьютерная преступность и компьютерная безопасность. М.: Юридическая литература, 1991. 160 с.
4. Бодэн Ж. Метод лёгкого познания истории. М.: Наука, 2000. 412 с.
5. Большая советская энциклопедия. Т. 25. М.: Большая советская энциклопедия, 1976. 600 с.
6. Бондаренко А., Маршалко Г., Шишкин В. ГОСТ Р 34.12–2015: чего ожидать от нового стандарта? // Information Security - Информационная безопасность. 2015. № 4. С. 48 - 50.
7. Ищукова Е.А., Богданов К.И. Реализация алгоритма шифрования Магма с использованием технологии NVidia Cuda // Международный журнал прикладных и фундаментальных исследований. 2015. №12. С. 789 - 793.

[58] Анненков А. В АП создана рабочая группа для координации работ по исполнению поручений о развитии Интернета в России – прошло первое заседание // Экспертный центр электронного государства. 11.02.2016. [Электронный ресурс]. URL: http://d-russia.ru/v-ap-sozdana-rabochaya-gruppa-dlya-koordinacii-rabot-po-ispolneniyu-poruchenij-o-razvitii-interneta-v-rossii-proshlo-pervoe-zasedanie.html (дата обращения: 07.10.2016).

[59] Анненков А. Подгруппа «Интернет+суверенитет» рабочей группы по Интернету рассмотрела проект дорожной карты // Экспертный центр электронного государства. 29.09.2016. [Электронный ресурс]. URL: http://d-russia.ru/podgruppa-internetsuverenitet-rabochej-gruppy-po-internetu-rassmotrela-proekt-dorozhnoj-karty.html (дата обращения: 07.10.2016).

[60] Доктрина информационной безопасности Российской Федерации (проект) // Совет Безопасности Российской Федерации. [Электронный ресурс]. URL: http://www.scrf.gov.ru/documents/6/135.html (дата обращения: 07.10.2016).

[61] Доктрина информационной безопасности Российской Федерации // Совет Безопасности Российской Федерации. [Электронный ресурс]. URL: http://www.scrf.gov.ru/documents/6/5.html (дата обращения: 07.10.2016).

8. Крапивенский А.С. Вербальный аспект культурной безопасности молодежи в социальных сетях и блогосфере рунета // Современные проблемы науки и образования. 2012. № 2. [Электронный ресурс]. URL: http://www.science-education.ru/ru/article/view?id=5935 (дата обращения: 04.12.2016).
9. Критически важные объекты и кибертерроризм. Часть 2. Аспекты реализации средств противодействия / О.О. Андреев, А.С. Шундеев, С.А. Афонин и др. Под ред. В.А. Васенина. М.: МЦНМО, 2008. 607 с.
10. Кучерявый М.М. Государственная политика информационного суверенитета России в условиях современного глобального мира // Управленческое консультирование. 2014. № 9. С. 7 - 14.
11. Малашевич Б.М. 50 лет отечественной микроэлектронике. Краткие основы и история развития. М.: Техносфера, 2013. 800 с.
12. Наумов А.О. Мягкая сила, цветные революции и технологии смены политических режимов в начале XXI века. М.: Аргамак-медиа, 2016. 274 с.
13. Таненбаум Э., Бос Х. Современные операционные системы. 4-е издание. М.: Питер, 2015. 1120 с.
14. Шиллер В.В., Шелудков Н.Н. Российские социальные сети как потенциальная угроза национальной безопасности России (на примере сайтов «Одноклассники» и «ВКонтакте») // Вестник Кемеровского государственного университета. 2013. № 1 (1). С. 124-129.
15. Штайншаден Я. Социальная сеть. Феномен Facebook. СПб.: Питер, 2011. 223 с.
16. Becker G.T., Regazzoni F., Paar C., and Burleson W.P. Stealthy Dopant-Level Hardware Trojans // Cryptographic Hardware and Embedded Systems – CHES. 2013. Vol. 8086 of the series Lecture Notes in Computer Science. Pp. 197 - 214.
17. Daemen J., Rijmen V. The Design of Rijndael, AES - The Advanced Encryption Standard. Springer-Verlag, 2002. 238 p.
18. Greenwald G. No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State. NY, Metropolitan Books, 2014. 304 p. [Электронный ресурс]. URL: http://us.macmillan.com/static/holt/greenwald/NoPlaceToHide-Documents-Uncompressed.pdf (дата обращения: 07.10.2016).
19. McMahon R., Bennett I. U.S. Internet Providers and the «Great Firewall of China» // Council on Foreign Relations. 23.02.2011. [Электронный ресурс]. URL: http://www.cfr.org/internet-policy/us-internet-providers-great-firewall-china/p9856 (дата обращения: 07.10.2016).
20. O'Neill J. Echelon: Somebody's Listening. Word Association Publishers, 2005. 345 p.
21. Paulson T.M. Intelligence Issues & Developm. Nova Publishers, 2008. 177 p.

Об авторе

Владислав Викторович Бухарин – к.и..н., старший преподаватель факультета государственного управления, МГУ имени М.В. Ломоносова, Москва, РФ. E-mail: Bukharin@spa.msu.ru.

THE RUSSIAN'S DIGITAL SOVEREIGNTY AS A TECHNICAL BASIS OF INFORMATION SECURITY

V.V. Bukharin

School of Public Administration, Lomonosov Moscow State University, Moscow, Russian Federation.

Abstract: *The article deals with the problem of the emergence of concept of "information sovereignty" in Russia, the prospects for its practical and theoretical introduction to the scientific revolution. The problem of "information sovereignty" in the normative documents of Russia, China and other Countries is examined. The focus of the article, first time in the domestic and foreign historiography, the technical aspects of independence in the field of digital technologies is analyzed. In this connection, the most important components of digital sovereignty is analyzed, technically ensuring national security. The author concludes that the main feature of the Russian technical resources to ensure the sovereignty of the information is fragmentary and uneven in the development of its components. The greatest progress has been made in the development of components such as the Russian search engines, social networks, national segment of "Internet" and the navigation system. Russian software and hardware require to ensure the accelerated development of information sovereignty, Russia's national security. The greatest attention should be Russian payment system, because this issue is directly dependent on the direction of development of the national economy. The problem of information sovereignty is largely related to issues of public decision-making, in bringing regulatory and legislative framework in line with the national security concept of the country.*

Key words: Information sovereignty, digital sovereignty, national security, information safety, import substitution.

References

1. Anureev S.V. *Platezhnye sistemy i ikh razvitie v Rossii* [Payment systems and their development in Russia]. Moscow, Finansy i statistika Publ., 2011. 288 p. (In Russian).
2. Baluev D.G. Vliianie sovremennykh sotsial'nykh media na informatsionnyi suverenitet Rossii: osnovnye podkhody k issledovaniiu [The impact of social media on information sovereignty of Russia: approaches to the study. State and municipal management]. *Gosudarstvennoe i munitsipal'noe upravlenie. Uchenye zapiski SKAGS,* 2015, no. 3, pp. 140 - 143. (In Russian).
3. Baturin Ju.M., Zhodzizhskij A.M. *Komp'juternaja prestupnost' i komp'juternaja bezopasnost'* [Computer crime and computer security]. Moscow, Iuridicheskaia literatura Publ., 1991. 160 p. (In Russian).
4. Bodjen Zh. Metod legkogo poznaniia istorii [Method for the easy knowledge of history]. Moscow, Nauka Publ., 2000. 412 p. (In Russian).
5. Bol'shaia sovetskaia entsiklopediia [The Great Soviet Encyclopedia]. Vol. 25. Moscow, Bol'shaia sovetskaia entsiklopediia, 1976. 600 p. (In Russian).
6. Bondarenko A., Marshalko G., Shishkin V. GOST R 34.12–2015: chego ozhidat' ot novogo standarta? [GOST R 34.12-2015: what to expect from the new standard?]. *Information Security - Informacionnaja bezopasnost',* 2015, no. 4, pp. 48 - 50. (In Russian).
7. Ishchukova E.A., Bogdanov K.I. Realizatsiia algoritma shifrovaniia Magma s ispol'zovaniem tekhnologii NVidia Cuda [Implementation of the encryption algorithm magma using NVidia CUDA technology]. *Mezhdunarodnyi zhurnal prikladnykh i fundamental'nykh issledovanii,* 2015, no. 12, pp. 789 - 793. (In Russian).
8. Krapivenskii A.S. Verbal'nyi aspekt kul'turnoi bezopasnosti molodezhi v sotsial'nykh setiakh i blogosfere runeta [Verbal aspect of youth cultural security in social networks and blogosphere of runet]. *Sovremennye problemy nauki i obrazovaniia,* 2012, no. 2. Available at: http://www.science-education.ru/ru/article/view?id=5935 (Accessed: 04.12.2016). (In Russian).
9. *Kriticheski vazhnye ob"ekty i kiberterrorizm. Chast' 2. Aspekty realizatsii sredstv protivodeistviia* [Crucial facilities and cyberterrorism. Part 2: Aspects of implementation of countermeasures]. O.O. Andreev, A.S. Shundeev, S.A. Afonin. Ed. by V.A. Vasenin. Moscow, MTsNMO Publ., 2008. 607 p. (In Russian).
10. Kucheryavyi M.M. Gosudarstvennaia politika informatsionnogo suvereniteta Rossii v usloviiakh sovremennogo global'nogo mira [State Policy Information Sovereignty Russia in Today's Global World]. *Upravlencheskoe konsul'tirovanie,* 2014, no. 9, pp. 7 - 14. (In Russian).
11. Malashevich B.M. *50 let otechestvennoi mikroelektronike. Kratkie osnovy i istoriia razvitiia* [50 years of domestic microelectronics. Brief history of the foundations and development]. Moscow, Tekhnosfera Publ., 2013. 800 p. (In Russian).
12. Naumov A.O. *Mjagkaja sila, cvetnye revoljucii i tehnologii smeny politicheskih rezhimov v nachale XXI veka* [Soft power, the color revolutions and the technology change of political regimes at the beginning of the XXI century]. Moscow, Argamak-media Publ., 2016. 274 p. (In Russian).
13. Tanenbaum A., Bos H. *Modern operating systems.* 4th edition. Prentice Hall, 2014. 1101 p. (Rus. Ed.: Tanenbaum A., Bos H. Sovremennye operatsionnye sistemy. 4th edition. Moscow, 2015. 1120 p.).
14. Shiller V.V., Sheludkov N.N. Rossiiskie sotsial'nye seti kak potentsial'naia ugroza natsional'noi bezopasnosti Rossii (na primere saitov «Odnoklassniki» i «VKontakte») [Russian social networking as a potential threat to Russian national security (example «Odnoklassniki» and «VKontakte»)]. *Vestnik Kemerovskogo gosudarstvennogo universiteta,* 2013, no. 1 (1), pp. 124 - 129. (In Russian).
15. Steinschaden Ja. *Phenomen Facebook: Wie eine Webseite unser Leben auf den Kopf stellt.* Carl Ueberreuter Verlag GmbH, 2010. 208 p. (Rus. ed.: Shtainshaden Ia. Sotsial'naia set'. Fenomen Facebook. Sankt-Peterburg, 2011. 223 p.).
16. Becker G.T., Regazzoni F., Paar C., and Burleson W.P. Stealthy Dopant-Level Hardware Trojans. *Cryptographic Hardware and Embedded Systems - CHES 2013,* vol. 8086 of the series Lecture Notes in Computer Science, pp. 197 - 214.
17. Daemen J., Rijmen V. *The Design of Rijndael, AES - The Advanced Encryption Standard.* Springer-Verlag, 2002. 238 p.
18. Greenwald G. *No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State.* New York, Metropolitan Books, 2014. 304 p. Available at: http://us.macmillan.com/static/holt/greenwald/NoPlaceToHide-Documents-Uncompressed.pdf (Accessed 07.10.2016).

19. McMahon R., Bennett I. U.S. Internet Providers and the «Great Firewall of China». *Council on Foreign Relations,* 23.02.2011. Available at: http://www.cfr.org/internet-policy/us-internet-providers-great-firewall-china/p9856 (Accessed 07.10.2016).
20. O'Neill J. *Echelon: Somebody's Listening*. Word Association Publ., 2005. 345 p.
21. Paulson T.M. *Intelligence Issues & Developm.* Nova Publ., 2008. 177 p.

About the author

Vladislav V. Bukharin – Ph.D., Senior Lecturer, School of Public Administration, Lomonosov Moscow State University, Moscow, Russian Federation. E-mail: Bukharin@spa.msu.ru.