Некоторые проблемы безопасности России в сфере информационных технологий

Разумовская Е.А.,
старший преподаватель кафедры
общегуманитарных и социально-экономических дисциплин
Санкт-Петербургского юридического института (филиала)
Академии Генеральной прокуратуры РФ, советник юстиции
E-mail: Razum_E@mail.ru

Аннотация. *В статье рассмотрены проблемы, связанные с зависимостью России от импорта компьютерной техники и программного обеспечения. Приведены статистические данные о соотношении отечественных и зарубежных производителей на рынке ИТ-технологий. Дан краткий обзор правового обеспечения курса России на импортозамещение в информационной сфере.*
Ключевые слова: *информационное пространство, информационная безопасность, защита персональных данных, программное обеспечение, импортозамещение.*

В настоящее время человечество находится на стадии перехода от постиндустриального к информационному обществу, в частности это проявляется в том, что существующие в реальности конфликты и противоречия переносятся в виртуальную сферу. Все развитые страны, так или иначе, защищают свое информационное пространство. В основном, вне закона оказывается контент трех видов: нарушающий авторские права, растлевающий детей, а также пропагандирующий экстремизм и терроризм. В глобальной сети действует немало преступных элементов, они распространяют вредоносные программы, шпионят, навязывают пользователям ненужные или несуществующие услуги, взламывают банковские счета. ИТ-преступность приносит ощутимый урон. Это актуальная и интересная тема, заслуживающая подробного исследования. Однако, по нашему мнению, в сфере информационных технологий России накапливаются еще более серьезные проблемы — это значительная, десятилетиями складывающаяся импортозависимость страны в компьютерной области.

По информации Федеральной службы государственной статистики, в 2013 г. в Россию было импортировано вычислительных машин и их блоков на 5791 млн долларов США, из них — на 4746 млн долларов — из дальнего зарубежья[1]. По данным портала выбора технологий и поставщиков TADVISER в 2013 г. на российский рынок было поставлено 10,24 миллиона стационарных и мобильных компьютеров[2]. В числе ведущих поставщиков зарубежные фирмы: Lenovo — 18 %, Acer — 14,8 %, Asus — 13,5 %. Лучшая отечественная компания по сборке компьютеров DNS заняла 5-е место с 3,6 %, она поставляет на рынок порядка 200 тыс. компьютеров в год. По свидетельству Национальной ассоциации инноваций и развития информационных технологий, сумма лицензионных отчислений, которые Россия платит зарубежным поставщикам программного обеспечения (ПО), составляет около 285 млрд руб. в год.

Однако до последнего времени ситуация не вызывала большой тревоги, при высоких ценах на углеводороды — основной предмет нашего импорта, мы закупали компьютерную технику и ПО во все возрастающих объемах. Но в 2014 г. ситуация поменялась кардинально, наступил период значительного снижения цены на нефть при одновременном вводе санкций против России. Опасность ситуации в экономике страны, потерявшей в 90-е гг. половину своего индустриального потенциала, подробно проанализирована в статье профессора В.В. Колесникова[3].

Рассмотрим более подробно проблемы безопасности и суверенитета России в области информационных технологий. Подавляющее число компьютеров в России, а в государственных учреждениях все 100 % работают под управлением операционной системы Windows, а в качестве стандартного офисного пакета используют MSOffice, разработанные американской фирмой Microsoft. Например, только зарегистрированных пользователей одной версии операционной системы Windows 7 в России порядка 10 млн. А теперь давайте предположим, что глубоко внутри операционных систем Windows имеются секретные закладки, в которых заложены скрытые деструктивные функции, например, команда на самоуничтожение, которую в любой момент могут активировать из США. Если это произойдет, в один момент выйдут из строя все компьютеры России на платформе Windows, имеющие выход в глобальную сеть. Поскольку никакой технической документации на Windows пользователям не предоставляется, а системные библиотеки

[1] URL: www.gks.ru (дата обращения: 16.05.2015).

[2] URL: www.tadviser.ru (дата обращения: 16.05.2015).

[3] См.: Колесников В.В. Национальная безопасность, глобализация и модель экономики // Вестник Санкт-Петербургского ун-та МВД России. 2014. № 4 (64). С. 136–144

не только многочисленны, но и хитроумно запутаны с точки зрения своего функционального предназначения, то очень легко спрятать там шпионский модуль, действующий по принципу «троянской программы», так называемый жучок. Описанная выше угроза является гипотетической, хотя и весьма вероятной. К сожалению, убедиться в ее реальности мы сможем только в самой критической ситуации, что еще больше усугубляет потенциальную опасность.

Другая же неприятность, следующая из сложившейся зависимости России от фирмы Microsoft и других производителей импортного ПО, состоит в том, что все мы (граждане, предприятия, организации, государственные учреждения) регулярно платим деньги за постоянное обновление программных продуктов. Коммерческая политика Microsoft направлена на обогащение за счет стран, где она находится в положении монополиста. Так, указанный производитель каждые два-три года выпускает новую версию операционной системы и пакета офисных программ, при этом перестают поддерживаться более ранние версии. Особую остроту ситуации придает то, что монополист специально выпускает все более и более ресурсоемкое ПО, заставляя пользователей массово менять компьютеры на более мощные задолго до выработки физического ресурса. Кроме того, операционную систему устанавливают теперь при сборке системного блока и заставляют пользователя платить за нее при покупке компьютера. Таким образом, мы все являемся заложниками финансовой политики Microsoft, Apple, Google, Oracle, Autodesk и других крупнейших американских фирм-производителей программного обеспечения и будем платить им миллиарды долларов, пока не преодолеем свою импортозависимость в этой сфере.

Международные правила лицензирования продукции, идущей на экспорт, разрабатывались исключительно с учетом интересов американских и транснациональных корпораций-монополистов. Что бы страна-производитель ни экспортировала — корабли, самолеты, вооружение, — продукция должна сопровождаться документаций, схемами, чертежами, подготовленными исключительно на лицензионном ПО. На заводах, в научных институтах, в конструкторских бюро России по их правилам должны быть установлены лицензионные программы от операционной системы до специальных программ конструирования, проектирования и дизайна. Кроме того, ведущие российские заводы для лицензирования своей продукции обязаны устанавливать у себя компьютерную систему управления предприятием для автоматизированного учета движения материальных ресурсов и финансовых средств, например, комплекс BAAN. Стоимость такого программно-аппаратного комплекса вместе с оборудованием превышает 1 млн долларов. Таким образом, любой выходящий на международный рынок производитель из России, желающий продать свою продукцию, облагается своеобразной данью со стороны монополий-производителей ПО.

Если производственные организации оказываются в кабале у зарубежных компаний на стадии оформления документации, то российские банки зависят от чужеземного программного обеспечения непосредственно в сфере своей основной и повседневной деятельности — это и система международных банковских переводов Swift, и пресловутые платежные системы Visa и MasterCard, отключением которых шантажируют Россию западные организаторы санкций.

Рассмотрим вопрос безопасности информационных технологий с точки зрения обороноспособности страны. Следует отметить, что в военной сфере давно осознали опасность использования американского ПО, там разработаны и продолжают разрабатываться автономные системы отечественного производства. Так, российская торпеда или ракета оснащается исключительно российским программным обеспечением, но, к сожалению, этот принцип пока не распространяется на научно-исследовательские институты и конструкторские бюро заводов, работающих на оборону страны. Возьмем, к примеру, область конструирования и проектирования. Самый популярный в России программный продукт в этой сфере — средство инженерного конструирования AutoCAD фирмы Autodesk, в России около 10 тыс. зарегистрированных корпоративных пользователей и миллионы индивидуальных, используется это ПО при проектировании зданий, конструировании кораблей, самолетов, подводных лодок и т.д. Компания Autodesk зарегистрирована в США и, подобно всем остальным американским производителям ПО, безоговорочно присоединилась к санкциям против России, более того, она заявила, что не намерена далее обеспечивать оборонный комплекс России своим программным продуктом.

Еще одна область информационных технологий, нуждающаяся в импортозамещении, — это средства управления базами данных (СУБД). В стране созданы и функционируют многочисленные банки и базы данных, в том числе в силовых ведомствах и правоохранительных органах. В качестве примеров действующих банков данных, содержащих миллионы записей, можно привести учеты МВД — базы данных зарегистрированных преступлений и преступников, лиц, пропавших без вести и находящихся в розыске, базы отпечатков пальцев и угнанного автотранспорта, хищений антиквариата и хищений из металлических хранилищ (сейфов) и т.д. В настоящее время в органах прокуратуры разрабатывается и внедряется

единая федеральная система учета преступлений «Государственная автоматизированная система Правовая статистика». Потенциальная угроза состоит в том, что указанная федеральная система, которая должна оказать существенное влияние на развитие правового государства в России, строится на основе СУБД Oracle американского производства. По данным портала выбора технологий и поставщиков TADVISER, рынок СУБД в России распределен между компаниями следующим образом: Oracle — 69,9 %, Microsoft — 8,5 %, IBM — 7,2 %, лучшая российская компания ВНИИНС — менее 0,4 % и разрабатывает ПО исключительно для военных нужд.

Существует еще одна потенциальная угроза для отечественных пользователей — мода на использование так называемых облачных технологий в сети Интернет, это новый популярный сервис, предоставляемый, например, офисными приложениями поисковой системы Google. С его помощью можно обращаться к своим документам и прочим файлам в любом месте, с любых устройств (стационарный компьютер, ноутбук, планшет, мобильный телефон). Информация пользователей при этом физически хранится на сервере корпорации Google в США. Таким образом, личные данные российских пользователей, коммерческие и производственные тайны, военные секреты могут стать достоянием иностранного государства.

По данным ВЦИОМ, в России 66 % граждан регулярно пользуются глобальной сетью Интернет, это около 95 млн чел.[4] Наши сограждане являются активными пользователями социальных компьютерных сетей, здесь соотношение в пользу отечественного программного продукта: ВКонтакте — 52,7 млн аккаунтов, Facebook–25,4 млн. Россияне размещают свои фотографии, домашнее видео, а также собственные заметки на зарубежных Интернет-ресурсах — YouTube, Twitter и тому подобных. Давно не является секретом, что через указанные порталы спецслужбы западных стран ищут и вербуют потенциальных агентов «пятой колонны», в том числе и в Российской Федерации.

Есть еще один аспект проблемы — чтение Интернет-сайтов пользователями осуществляется под управлением программ-браузеров, самые распространенные в России — Internet Explorer (в составе Windows), Google Chrome, Mozilla Firefox, Opera, — все они импортного производства. Кроме того, программирование серверов для создания сайтов производится на специальном языке PHP (Personal Home Page Tools), который сам написан на языке программирования C++ американской компании Bell Labs. Если предположить, что в системных библиотеках C++ заложены скрытые деструктивные функции, то во власти американских разработчиков будет в любой момент полностью обрушить сеть Интернет в России. Это может привести к непредсказуемым последствиям, как экономического, так и социального характера, возникнет хаос в системе управления, нарушится порядок деятельности государственных органов власти.

В последнее время руководство Российской Федерации ставит все более амбициозные задачи по компьютеризации страны, один из недавних примеров — предложение премьер-министра по полному переводу в электронную форму врачебной документации, выписывание электронных больничных и т.д. Единые для страны базы данных создаются, чтобы ими можно было пользоваться в режиме on-line из любого региона, при этом основной способ передачи данных — по сети Интернет. Кодирование и шифрование не дает стопроцентной гарантии безопасности, кроме того, большинство программ для шифрования — тоже импортного производства.

Несмотря на перечисленные угрозы безопасности компьютерной сфере России, не может быть и речи об отказе от компьютерных технологий, поскольку это существенно затормозит развитие страны. Но и оставаться в полной зависимости от американских производителей ПО в нынешних непростых условиях означает потерю суверенитета в области компьютерных технологий и, следовательно, угрозу информационной составляющей национальной безопасности. Остается, по нашему мнению, только одна разумная альтернатива — развивать свое собственное ПО. В этой связи можно процитировать «Стратегию национальной безопасности Российской Федерации до 2020 года», утвержденную Указом Президента РФ от 12.05.2009 № 537. В частности, в п. 61 гл. IV «Обеспечение национальной безопасности» говорится, что для противодействия угрозам экономической безопасности государственная социально-экономическая политика должна быть направлена на развитие индустрии информационных и телекоммуникационных технологий, средств вычислительной техники, радиоэлектроники, телекоммуникационного оборудования и программного обеспечения.

Область информационных технологий, в частности Интернет-технологий, в России — одна из самых быстро развивающихся отраслей, по данным Федеральной службы государственной статистики, оборот ИТ-сервисов в 2013 г. составил более 363 млрд руб., это 9,6 % от общего объема инновационных товаров, работ, услуг, и этот процент год от года растет. Ведущие вузы России выпускают высококлассных программистов, в стране есть кадровые ресурсы и оборудование для создания современного отечественного ПО, нужны организационные усилия и помощь со стороны государства.

[4] URL: www.wciom.ru (дата обращения: 16.05.2015).

Безопасность страны в сфере информационных технологий в 2014 г. стали предметом внимания высшего руководства страны. В июле 2014 г. по поручению Президента РФ Минкомсвязь России при участии Минобороны, ФСБ и других ведомств провело учения, направленные на выработку мер по предотвращению нарушений работы сети Интернет на территории России в результате негативного целенаправленного воздействия. В мае 2015 г. Президент РФ подписал Указ № 260 «О некоторых вопросах информационной безопасности Российской Федерации», который ставит перед ФСО РФ задачу организации до 31.12.2017 г. российского сегмента Интернета и подключения к нему по защищенным каналам информационных систем, находящихся в ведении государственных органов.

В июле 2014 г. в Федеральный закон «О персональных данных» были внесены изменения, которые вступят в силу с 01.09.2015 г. В частности, в ст. 18 гл. 4 добавлена ч. 5, которая обязывает операторов при сборе персональных данных посредством информационно-телекоммуникационной сети Интернет использовать серверы, находящиеся на территории Российской Федерации.

Летом 2014 г. депутаты Государственной Думы России начали готовить поправки в Федеральные законы от 18.07.2011 № 223-ФЗ «О закупках товаров, работ, услуг отдельными видами юридических лиц» и от 05.04.2013 № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд», которые делают приоритетными закупки отечественного ПО.

Национальная ассоциация инноваций и развития информационных технологий в рамках реализации программы импортозамещения сообщила о законодательном закреплении обязанности Правительства РФ обеспечить ведение специального реестра программного обеспечения силами профильных ведомств. В сентябре 2014 г. министр связи и массовых коммуникаций РФ предложил проект создания отдельного целевого фонда по развитию российского программного обеспечения, формируемого за счет специального сбора в размере 10 % на продаваемое в России ПО, 3/4 из которого зарубежного производства. Президент РФ поддержал идею создания фонда и поручил проработать этот вопрос в Правительстве РФ.

Развитие специального ПО в России могло бы поддерживаться ведомствами и организациями, заинтересованными в компьютеризации своей деятельности, а создание ПО общего назначения — финансироваться государством в рамках целевой комплексной программы. По мере продвижения к информационному обществу доля информационных продуктов и технологий будет возрастать, поэтому обеспечение безопасности и суверенитета в информационной сфере будет означать укрепление суверенитета страны в целом.

Список литературы:

1. Колесников В.В. Национальная безопасность, глобализация и модель экономики // Вестник Санкт-Петербургского ун-та МВД России. 2014. № 4 (64). С. 136–144.
2. Коршунова О.Н., Разумовская Е.А. Некоторые проблемы обеспечения безопасности информации // Юридическая мысль. 2014. № 2 (82). С. 83–91.

Some security problems of Russia in the field of information technology

Razumovskaya E.A.,
Senior lecturer of the Department of General humanitarian
and socio-economic disciplines of the St. Petersburg law Institute (branch)
of the Academy of prosecution General of the Russian Federation, Counsellor of justice
E-mail: Razum_E@mail.ru

Abstract. *The article considers the problems associated with the dependence of Russia on import of computer hardware and software. Shows statistics on the ratio of domestic and foreign manufacturers on the market of it technologies. A brief overview of the legal enforcement of course of Russia on import substitution in the information sphere.*
Keywords: *information space, information security, personal data protection, software, import substitution.*

References:

1. Kolesnikov V.V. Nacional'naja bezopasnost', globalizacija i model' jekonomiki // Vestnik Sankt-Peterburgskogo un-ta MVD Rossii. 2014. № 4 (64). S. 136–144.
2. Korshunova O.N., Razumovskaja E.A. Nekotorye problemy obespechenija bezopasnosti informacii // Juridicheskaja mysl'. 2014. № 2 (82). S. 83–91.