УДК 339.5

ПЕРСПЕКТИВЫ ВНЕДРЕНИЯ ИМПОРТОНЕЗАВИСИМОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ В ДЕЯТЕЛЬНОСТЬ ТАМОЖЕННЫХ ОРГАНОВ КАК УСЛОВИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Коды JEL: F13

Минакова И. В., *доктор экономических наук, профессор, декан факультета государственного управления и международных отношений, Юго-Западный государственный университет, г. Курск, Россия*
E-mail: irene19752000@mail.ru; SPIN-код: 8703-5224

Бабаскина О. В., *доцент кафедры таможенного дела и мировой экономики, Юго-Западный государственный университет, г. Курск, Россия*
E-mail: ola2306@yandex.ru; SPIN-код: отсутствует

Деркач Н. Е., *кандидат экономических наук, доцент, заведующий кафедрой таможенного дела и мировой экономики, Юго-Западный государственный университет, г. Курск, Россия*
E-mail: tavag5@yandex.ru; SPIN-код: 6096-8004

Поступила в редакцию 31.07.2024. Принята к публикации 14.08.2024

Аннотация

Актуальность темы. *Конкурентоспособность национальной экономики в значительно степени определяется эффективностью реализуемой таможенной политики и таможенного администрирования в условиях современных реалий. Сохраняющийся в настоящее время уровень активности деструктивных воздействий, направленных на дестабилизацию деятельности государственных органов России, в том числе Федеральной таможенной службы, требует поиска продуктивных решений по обеспечению их информационной безопасности. Одним из факторов, непосредственно влияющих на стабильность работы используемых информационно-технических средств, является зарубежное информационно-техническое обеспечение, которое, зачастую несет в себе скрытые возможности для негативного воздействия как на функционирование программных и аппаратных средств, так и на сохранность информации, консолидированной и обрабатываемой в процессе выполнения функционала теми или иными государственными органами и организациями. В связи с чем появляется объективная необходимость перехода на отечественные программные продукты различной функциональной направленности.*

Цель. *Системное исследование возможностей перехода Федеральной таможенной службы России на отечественные операционные системы и программные продукты различной функциональной направленности, выступающего важнейшим условием качественной защиты ее внутренних информационно-технических ресурсов и обеспечения экономической безопасности государства.*

Методология. *Методология исследования опирается на системный и процессный подходы. В ходе исследования использованы общенаучные и специальные приемы и методы познания: системный анализ и синтез, индукция, дедукция, теоретическое моделирование, формально-логический метод, методы построения гипотез, интерпретация правовых концепций и нормативных правовых актов.*

Результаты и выводы. *Авторами осуществлен системный анализ информационных ресурсов таможенных органов Российской Федерации с позиций обеспечения информационной безопасности. Оценены перспективы внедрения российского программного и аппаратного обеспечения, удовлетворяющего основным требованиям по информационной безопасности, отказоустойчивости, производительности и скорости обработки информации, осуществления архивирования и оптимизации хранимой информации, осуществления качественного анализа больших объемов данных при выполнении всего функционала таможенных органов.*

Область применения. *Сформулированные теоретические положения могут быть использованы в рамках процесса импортозамещения программного обеспечения деятельности таможенных органов Российской Федерации.*

Ключевые слова: *импортозамещение, информационная безопасность, цифровая трансформация, таможенные органы.*

Публикация выполнена в рамках государственного задания на 2024 год № 0851-2020-0034

UDC 339.5

PROSPECTS OF INTRODUCING IMPORT-INDEPENDENT SOFTWARE IN THE ACTIVITIES OF CUSTOMS AUTHORITIES AS A CONDITION OF INFORMATION SECURITY

JEL Codes: F13

Minakova I. V., *Doctor of Economics, Professor, Dean of the Faculty of Public Administration and International Relations, Southwestern State University, Kursk, Russia*
E-mail: irene19752000@mail.ru; SPIN-code: 8703-5224

Babaskina O. V., *Associate Professor of the Department of Customs and World Economy, Southwestern State University, Kursk, Russia*
E-mail: ola2306@yandex.ru; SPIN-code: missing

Derkach N. E., *PhD in Economics, Associate Professor, Head of the Department of Customs and World Economy, Southwestern State University, Kursk, Russia*
E-mail: tavag5@yandex.ru; SPIN-code: 6096-8004

Abstract

Relevance of the topic. *The competitiveness of the national economy is significantly determined by the effectiveness of the implemented customs policy and customs administration in the conditions of modern realities. The current level of activity of destructive influences aimed at destabilising the activities of Russian state bodies, including the Federal Customs Service, requires the search for productive solutions to ensure their information security. One of the factors directly affecting the stability of the work of the used information and technical means is foreign information and technical support, which often carries hidden opportunities for negative impact both on the functioning of software and hardware, and on the safety of information consolidated and processed in the process of performing the functionality of these or those state bodies and organisations. In this connection there is an objective necessity of transition to domestic software products of different functional orientation.*

Goal. *Systematic study of the possibilities of transition of the Federal Customs Service of Russia to domestic operational systems and software products of different functional orientation, which is the most important condition for the quality protection of its internal information-technical resources and ensuring the economic security of the state.*

Methodology. *The research methodology is based on system and process approaches. In the course of the research general scientific and special techniques and methods of cognition were used: system analysis and synthesis, induction, deduction, theoretical modelling, formal-logical method, methods of hypothesis construction, interpretation of legal concepts and normative legal acts.*

Results and conclusions. *The authors carried out a system analysis of information resources of customs authorities of the Russian Federation from the position of information security. The prospects of implementation of the Russian software and hardware that meets the basic requirements for information security, fault tolerance, performance and speed of information processing, archiving and optimisation of stored information, quality analysis of large amounts of data in the performance of the entire functionality of customs authorities have been assessed.*

Scope of application. *The formulated theoretical provisions can be used within the process of import substitution of software for the activities of customs authorities of the Russian Federation.*

Keywords: *import substitution, information security, digital transformation, customs authorities.*

The publication was carried out within the framework of the State Task for 2024 № 0851-2020-0034.

DOI: 10.22394/1997-4469-2024-66-3-70-80

Введение

Конкурентоспособность национальной экономики в значительно степени определяется эффективностью реализуемой таможенной политики и таможенного администрирования в условиях современных реалий. Сохраняющийся в настоящее время уровень активности деструктивных воздействий, направленных на дестабилизацию деятельности государственных органов России, в том числе Федеральной таможенной службы, требует поиска продуктивных решений по обеспечению их информационной безопасности. Одним из факторов, непосредственно влияющих на стабильность работы используемых информационно-технических средств, является зарубежное информационно-техническое обеспечение, которое, зачастую несет в себе скрытые возможности для негативного воздействия как на функционирование программных и аппаратных средств, так и на сохранность информации, консолидированной и обрабатываемой в процессе выполнения функционала теми или иными государственными органами и организациями. В связи с чем появляется объективная необходимость перехода на отечественные программные продукты различной функциональной направленности.

Правильный подбор, тестирование и внедрение российского программного обеспечения позволит решить значительную часть проблемы обеспечения информационной безопасности критически важной инфраструктуры России.

Целью данной работы выступает системное исследование возможностей перехода Федеральной таможенной службы России на отечественные оперативные системы и программные продукты различной функциональной направленности, выступающего важнейшим условием качественной защиты ее внутренних информационно-технических ресурсов и обеспечения экономической безопасности государства.

Методология исследования опирается на системный и процессный подходы. В ходе исследования использованы общенаучные и специальные приемы и методы познания: системный анализ и синтез, индукция, дедукция, теоретическое моделирование, формально-логический метод, методы построения гипотез, интерпретация правовых концепций и нормативных правовых актов.

Информационную базу исследования определили нормативные правовые акты Евразийского экономического союза, федеральные законы, подзаконные акты, концепции, национальные и федеральные проекты, дорожные карты и программы социально-экономического развития Российской Федерации, нормативные правовые акты ФТС России, аналитические и статистические материалы ФТС России, публикации в научных периодических изданиях по исследуемой проблематике, информация официальных сайтов федеральных органов власти и аналитических материалов, представленных в сети Интернет.

Анализ проблем обеспечения информационной безопасности организаций и обоснование необходимости перехода на отечественное программное обеспечение

В декабре 2016 г. главы государств-членов Евразийского экономического союза (далее — ЕАЭС) подписали «Заявление о цифровой повестке ЕАЭС» [1], в котором правительствам государств-членов ЕАЭС совместно с Евразийской экономической комиссией (далее — ЕЭК) было дано поручение разработать до 1 декабря 2017 года и представить для рассмотрения Евразийским межправительственным советом Основные направления реализации цифровой повестки ЕАЭС до 2025 га. Данное событие положило начало законодательной деятельности по разработке «цифровых платформ» в рамках ЕАЭС, стало основополагающим для реализации различных проектов по цифровизации, цифровому трансформированию различных национальных институтов, в том числе и таможенной службы России, с дальнейшей перспективой реализации взаимных интеллектуально-технических решений в рамках ЕАЭС. За время реализации различных цифровых проектов, принимаемых с 2017 г., видение цифровизации деятельности органов исполнительной власти, в частности, Федеральной таможенной службы России (далее — ФТС России), постепенно изменяется. Прогресс в информационно-технической сфере (IT-сфере) за последние годы в значительной степени влияет на трансформацию первоначально принятых решений и проектов, в связи с чем, ФТС России постоянно вносит коррективы в Программу ведомственной цифровизации.

С начала специальной военной операции (далее — СВО) санкционное давление на Россию, связанное, в том числе, с ограничениями в использовании зарубежных информационно-технических и программных систем, показало, что необходимость замещения информационных платформ отечественными аналогами является жизненно необходимым для обеспечения работоспособности различных федеральных органов исполнительной власти (далее — ФОИВ) и государственных компаний России, защиты внутренней информации российских организаций и ведомств, а также данных, используемых при выполнении функционала решаемых ими задач.

Цифровизация деятельности ФОИВ, в число которых входит ФТС России, непосредствен-

но связана с такими принципами, как импортозамещение и информационная безопасность, необходимость и актуальность применения которых при реализации цифровых программ становится всё более насущными.

Современные тенденции применения IT не представляются без использования искусственного интеллекта и больших массивов данных (Big Data), что, в свою очередь, предъявляет повышенные требования к информационной безопасности (далее — ИБ), скорости обработки баз данных (далее — БД), техническим требованиям к используемому оборудованию.

Отметим, что с начала применения таможенными органами возможностей электронного интернет-декларирования, система обмена информацией между ФТС России и участниками внешнеэкономической деятельности (далее — ВЭД) претерпела значительные изменения [2]. Изменилась, в том числе, и структура таможенных органов.

Перемещение электронного декларирования в региональные Центры электронного декларирования (далее — ЦЭД) привело к переориентации информационно-цифровых потоков данных посредством ведомственной интегрированной телекоммуникационной сети (далее — ВИТС), а также изменило нагрузку на её составляющие. Что, в частности, показало слабые стороны применяемых систем анализа больших массивов данных, недостатки применяемых таможенными органами информационно-вычислительных средств и систем, а также повысило требования к сохранности и достоверности данных.

При этом очевидной стала необходимость по решению следующих вопросов:

1) проблем, возникающих при консолидировании и анализе таможенной информации, а именно: скорости обработки данных из больших массивов, осуществления выборок информации за значительные временные промежутки, а также скорости передачи информации;

2) кибербезопасности (как всей системы в целом, так и отдельных её звеньев) — существенной составляющей любой информационно-технической системы, влияющей на сохранность и достоверность данных, на всех этапах осуществления задач посредством информационно-технического потенциала, а также при использовании различных информационно-аналитических систем.

С началом СВО актуальность вопросов информационной безопасности стала наиболее актуальной. О существенном влиянии данного направления на деятельность ФОИВ РФ может говорить тот факт, что после 24 февраля 2022 г. были изданы несколько законодательных актов, направленных на упрочение позиций в области информационной безопасности, среди которых:

1) Приказ Министерства цифрового развития, связи и массовых коммуникаций России от 10.03.2022 г. № 186 «Об утверждении Методических рекомендаций по обеспечению необходимого уровня безопасности в сфере информационно-коммуникационных технологий государственных корпораций, компаний с государственным участием, а также их дочерних организаций и зависимых обществ» [3];

2) Указ Президента Российской Федерации от 01.05.2022 г. № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации» [4, 5];

3) Постановление Правительства Российской Федерации от 15.07.2022 г. № 1272 «Об утверждении типового положения о заместителе руководителя органа (организации), ответственном за обеспечение информационной безопасности в органе (организации), и типового положения о структурном подразделении в органе (организации), обеспечивающем информационную безопасность органа (организации)» [6];

4) Распоряжение Правительства РФ от 22.12.2022 г. № 4088-р «Об утверждении Концепции формирования и развития культуры информационной безопасности граждан Российской Федерации» [7];

5) Указ Президента РФ от 12.04.2021 № 213 «Об утверждении Основ государственной политики Российской Федерации в области международной информационной безопасности» [8, 5];

6) Приказ Министерства цифрового развития, связи и массовых коммуникаций России от 18.01.2023 г. № 21 «Об утверждении Методических рекомендаций по переходу на использование российского программного обеспечения, в том числе на значимых объектах критической информационной инфраструктуры Российской Федерации, и о реализации мер, направленных на ускоренный переход органов государственной власти и организаций на использование российского программного обеспечения в Российской Федерации» [9].

Отметим, что нами приведены лишь некоторые нормативно-правовые акты, призванные активизировать деятельность в сфере обеспечения кибербезопасности. Данный неполный перечень свидетельствует о важности анализируемых проблем.

В 2023 г. российская таможня столкнулась с атаками на свою ИТ-систему со стороны украинских, европейских, американских и других хакерских групп, имеющих цель максимально дестабилизировать цифровые платформы ФОИВ России. По данным временно исполняющего обязанности (далее — врио) руководите-

ля ФТС России Р. В. Давыдова, с февраля 2022 г. на ресурсы ФТС России в среднем идет по три-четыре DDoS-атаки ежедневно, по состоянию на 25 октября 2023 г. количество внешних деструктивных воздействий превысило 1500 [10].

С 10 по 12 апреля 2023 г. вследствие мощнейших кибератак наблюдались сбои в работе ЕАИС ТО, а ФТС России пришлось остановить работу электронных таможенных сервисов и перейти на бумажный документооборот [11]. Учитывая, что, согласно данным ФТС России, показатель «Доля деклараций на товары, оформленных в электронном виде без представления документов на бумажном носителе, в общем количестве оформленных деклараций на товары при условии, что товары (транспортные средства) не идентифицированы как рисковые поставки, требующие дополнительной проверки документов на бумажных носителях (процентов)» с 2015 г. не снижался ниже значения 99,2 % [10], то переход к бумажному документообороту говорит о значительности происшедшего в апреле 2023 г. деструктивного воздействия на информационно-техническую структуру ФТС. Продолжительность воздействия данного инцидента официально продолжалось до 21 апреля 2023 г.

Как указывает в своем исследовании М. В. Ионина, ФТС России пришлось пересмотреть текущий подход к организации информационной безопасности, в связи с произошедшим дестабилизирующим воздействием на основные бизнес-процессы, которое привело к «приостановке, либо к полной блокировке функционирования» [12, с. 48].

Применение в современной деятельности таможни информационных систем, основанных на платформе Windows, может быть одним из факторов проблемы информационной безопасности, связанным с «пробелами», заложенными в её основе. Перспективы перехода на использование исключительно российского программного обеспечения, базирующего на операционной системе Astra Linux, как считают эксперты, может в значительной степени снизить риски влияния извне на таможенные базы данных и системы, а также существенно укрепить безопасность информационно-технической составляющей деятельности таможенных органов России.

1 декабря 2023 г. на заседании коллегии ФТС России врио руководителя ФТС России Р. В. Давыдов говоря о дальнейших планах цифрового развития ФТС России, сообщил о планах по введению в промышленную эксплуатацию в 1 квартале 2024 г. Главного центра обработки данных в Твери (ГЦОД «Тверь»), куда будут перенесены основные информационно-технические ресурсы из г.Москвы (объект «Фили» ФТС России), в связи с чем будет организован «процесс миграции всех информационно-программных средств, автоматизирующих процессы таможенного дела» [10]. Предположительно ГЦОД «Тверь» позволит хранить 25 петабайт, т. е. в 1,5 раза больше, чем позволяют текущие мощности серверов ЦИТТУ ФТС России. В рамках долгосрочных перспектив, Р. В. Давыдов отметил, что на базе ГЦОД «Тверь» в течении следующего пятилетия «планируется развертывание отдельного экземпляра Единой цифровой платформы РФ «ГосТех»» [10].

Создание единой цифровой платформы РФ «ГосТех» было инициировано Правительством РФ 12 октября 2020 г. [13] с перспективой, что она станет фундаментом для дальнейшего совершенствования всех государственных информационных технологий на основе отечественных цифровых решений. Постановлением Правительства РФ от 16 декабря 2022 г. №2338 утверждено «Положение о единой цифровой платформе Российской Федерации «ГосТех»» [14].

Необходимо отметить, что помимо платформы «ГосТех», которая включает «облачные» сервисы, в настоящее время активно развивается инфраструктурная облачная платформа «Гособлако», которая может стать как конкурентом, так и дополнением функционала «ГосТех». При этом основой обоих платформ заявлено применение исключительно отечественного программного обеспечения, включая операционные системы, системы обработки информации, системы защиты информационной безопасности.

В ходе мероприятий Международного форума «Технология и безопасность», проходивших в очном формате с 13 по 15 февраля 2024 г. особое внимание было уделено проблемам цифровой трансформации (6 тематических мероприятий) и информационной безопасности (5 тематических мероприятий).

Начальник 9 управления Федеральной службы по техническому и экспортному контролю (далее — ФСТЭК России) С. В. Бондаренко в своем выступлении регламентировал основные причины уязвимости информационных систем организаций перед хакерскими атаками, в которые входят: слабые пароли пользователей и администраторов, однофакторная идентификация и использование паролей, установленных по умолчанию, оказались на вершине списка [15].

В качестве первоочередных мер защиты информации С. В. Бондаренко предложил следующие: инвентаризация информационных ресурсов; антивирусная защита рабочих мест; защита периметра информационной инфраструктуры; управление доступом пользовате-

лей; мониторинг событий информационной безопасности; контроль почтовых вложений на предмет наличия вредоносного программного обеспечения; очистка входящего из сети «Интернет» трафика.

В своем выступлении на Форуме заместитель директора ФСТЭК России В. С. Лютиков презентовал основные направления совершенствования технической защиты информации, в числе которых предусмотрены, в том числе и мероприятия по информационной безопасности при внедрении систем искусственного интеллекта, системного программного обеспечения, повышение защищенности от DdoS-атак [15].

Необходимо отметить, что в ФТС России на момент успешных хакерских атак в апреле 2023 г. было реализовано большинство превентивных мероприятий, предложенных С. В. Бондаренко. Это позволяет предположить, что основным фактором, отрицательно повлиявшим на систему безопасности ЕАИС ТО, выступила именно скрытая «уязвимость» иностранного программного обеспечения. В связи с чем переход к отечественному программному обеспечению, начиная от операционных систем, как серверных, так и пользовательских, и заканчивая офисными программами, при условии соблюдения всех мер технической защиты, рекомендованных ФСТЭК России, может в значительной степени повысить устойчивость «цифровой» составляющей ФОИВ, и, в частности, ФТС России.

Современное развитие потенциала отечественных программных решений позволяет осуществить эффективный переход с применяемых иностранных систем на отечественные аналоги. Однако при этом возникает множество дополнительных требований, без реализации которых данный переход невозможен [16]. В связи с чем, необходимо тесное взаимодействие ФТС России с организациями, которые в настоящее время осуществляют реализацию аналогичных проектов, на предмет возникающих при этом технических, технологических и иных вопросов, связанных с обучением персонала, сохранностью имеющейся в системах информации, возможностями обработки архивных и новых данных и их совмещения, защитой информации, в том числе информационных потоков данных в режиме on-line, эффективной обработкой больших массивов данных, с учетом одновременной работы множества процессов на одном массиве информации, профилактикой и сохранением резервных копий БД, с учетом их постоянной пополняемости и работы ЕАИС ТО в режиме 24/7.

Согласно данным официального сайта автономной некоммерческой организация «Центр компетенций по импортозамещению в сфере информационно-коммуникационных технологий» (далее — АНО «ЦКИТ»), по «Результатам мониторинга закупок программного обеспечения для обеспечения государственных и муниципальных нужд по состоянию на 01.01.2023» [18] в 2022 г. в количественном выражении доля закупок отечественного программного обеспечения составила 87,08 %, (иностранного — 7,34 %), при этом, доля финансовой составляющей российского программного обеспечения составляет 54,19 % (доля иностранного — 27,77 %) [18].

Таким образом, соотношение долей количественного и денежного выражения в закупках программных продуктов отечественного и иностранного происхождения позволяет сделать вывод о том, что важность перехода на отечественное программное обеспечение обусловливается не только необходимостью ограничения вероятного использования потенциала иностранных программных продуктов для кражи информации государственных компаний, ФОИВ, муниципальных органов власти, возможности манипулировать данными ресурсами, используя скрытые «триггеры», но оказывается финансово привлекательным для бюджета.

На сайте Центра компетенций по импортозамещению в сфере ИКТ представлен Каталог, содержащий список отечественных программных разработок для замещения иностранных программных продуктов [19] (на 20.02.2024 г. содержит 6285 записей), в котором представлены иностранные программные продукты и варианты отечественных «заменителей», а также области их применения.

Обзоры российского интернет-портала аналитического агентства «Tadviser» «Государство. Бизнес. Технологии» [19, 20] по проектам импортозамещения программного обеспечения, начатым в различных органах и организациях РФ с 2015 г., позволяют выбрать вероятностные продукты, опыт перехода на которые можно исследовать посредством обмена информации с другими ведомствами и, в случае его эффективности и приемлемости для решения задач, стоящих перед ФТС России, рассмотреть вероятность его практического применения.

Учитывая, что, как указывается в обзоре «Tadviser», «среди представленных кейсов чаще всего происходит миграция с продуктов трех вендоров — Microsoft, SAP и Oracle» [21], а в ФТС России наиболее применимы продукты Microsoft и Oracle, необходимо присмотреться к отечественным (или open source) решениям, преобладающим при переходе различных крупных компаний и организаций с подразделениями, находящимися по всей территории РФ и решающих задачи, связанные с обработкой больших массивов данных в режиме on-line 24/7.

В результате анализа, проведенного Tadviser наиболее частым замещением СУБД Oracle является СУБД PostgreSQL/Postgres Pro, что позволяет говорить о целесообразности исследования возможностей данного продукта с условием перехода с операционной системы Microsoft на платформу Astra Linux.

Опубликованные Министерством цифрового развития, связи и массовых коммуникаций Российской Федерации в январе 2024 г. «Методические рекомендации по цифровой трансформации государственных корпораций и компаний с государственным участием» регламентируют сроки перехода на отечественные программные ресурсы государственных компаний, а именно необходимость применения ими российских операционных систем, офисных пакетов, антивирусов, систем виртуализации — с 1 января 2025 г.; отечественных систем управления базами данных — с 1 января 2026 г. [3].

Необходимо отметить, что среди проектов импортозамещения программного обеспечения, стартовавших в 2015—2023 гг., представленных в аналитических статьях на сайте https://www.tadviser.ru, единственным проектом ФТС указан проект замещения «Телекоммуникационное оборудование Cisco» на отечественный аналог (Телекоммуникационное оборудование «Элтекс» и «Фактор-ТС»), начатый в 2017 г. по контрактам, заключенным ФТС России с Инлайн технолоджис, Ситек, Н-ком (Замещение телекоммуникационного оборудования Cisco отечественными решениями (учтено 4 контракта)).

Если рассматривать проекты импортозамещения, начатые в 2022—2023 гг., то, учитывая актуальность аналогичных решений, необходимых для ФТС России, обращают на себя внимание следующие [22, 21]:

1) ФНС России (2023 г.) — замещение СУБД и ОС от Oracle и Microsoft на российские ОС и СУБД;

2) Казначейство России (2023 г.) — замещение СУБД Oracle на отечественное или open source решение (СУБД Postgres Pro);

3) Гознак (2022 г.) — замещение Microsoft SQL Server на отечественное или open source решение (СУБД Postgres Pro);

4) Администрация Курской области (2022 г.) — замещение Microsoft Office на отечественное или open source решение («МойОфис»);

5) Магнитогорский металлургический комбинат (2022 г.) — замещение Oracle на отечественное или open source решение (Visary Project);

6) Россети (2023 г.) — замещение SAP на отечественное или open source решение (Импортонезависимая система на базе отечественного ПО, а именно Системе управления производственными активами (СУПА), которая предназначена для автоматизации, оптимизации и унификации бизнес-процессов),

7) НИТИ им. Александрова (2022 г.) — замещение MS SQL Server на отечественное или open source решение (PostgreSQL, Astra Linux);

8) ФГБУ «РЭА» Минэнерго России (2022 г.) — замещение Иностранные BI-системы на отечественное или open source решение (Платформа ТриВи 3V).

Исходя из этого, помимо изучения аналитических обзоров программных продуктов, регулярно размещаемых коммерческими и некоммерческими организациями, необходимо организовать сотрудничество по обмену опытом между отечественными ФОИВ, муниципальными образованиями, государственными организациями (например, Казначейство России, Гознак, ФНС России и др.), организациями, предоставляющими услуги связи, крупными российскими банками для обмена информацией по результатам внедрения отечественных операционных систем, СУБД и программного обеспечения на предмет выявления их «сильных» и «слабых» сторон, защищенности данных от внешнего воздействия, возможности быстрой адаптации имеющегося программного обеспечения организаций к новым системам и переноса данных на новые информационно-программные платформы.

Импортозамещение широко применяемых операционных систем иностранного производства (в частности, Windows) на отечественное программное обеспечение в настоящее время жизненно необходимо для снижения отрицательного воздействия от хакерских атак, использующих заложенные в коде Windows и других известных иностранных информационных систем уязвимости.

Учитывая публикации интернет-портал по информационной безопасности в сети (https://safe-surf.ru/) [23, рассчитанные как на специалистов по информационной безопасности, так и на рядовых пользователей, а также бюллетени Национального координационного центра по компьютерным инцидентам (далее — НКЦКИ) с уведомлениями об угрозах информационной безопасности, обращают на себя внимание многочисленные новости об устранении уязвимостей в программных продуктах ведущих иностранных разработчиков программного обеспечения. Данный факт также является косвенным подтверждением вероятности преднамеренного включения аналогичных «уязвимостей», направленных на дестабилизацию работы организаций и похищение критически важной информации в целях иностранных разведок. Как указывает в своей статье П. Гончаров (заместитель директора по развитию биз-

неса Solar JSOC (Центр мониторинга и реагирования на инциденты информационной безопасности компании «Ростелеком» - https://rt-solar.ru/)) для любого центра мониторинга информационной безопасности (SOC) актуальными являются проблемы, включающим в себя:

— кадры — обусловлена нехваткой специалистов высокого уровня по осуществлению информационной безопасности организации;

— технологии — необходимость и актуальность полного перехода на отечественные программные продукты, причем не только в области защиты данных;

— процессы — в настоящее время стремление к деструктуризации работы отечественных организаций, банков, компаний наблюдается практически повсеместно, кроме того, каждая десятая компания-субъект критической информационной инфраструктуры заражена каким-то видом вредоносного программного обеспечения [11].

Заключение

На примере таможенных органов совершенно очевидно, что при реализации «реорганизации» используемой операционной системы актуальными становятся проблемы по переводу на новые операционные системы, адаптации к ним всех имеющихся в таможенных органах автоматизированных, информационно-аналитических, информационно-справочных систем, различных комплексов программного обеспечения, систем управления базами данных, а также многочисленных и весьма значительных по объему баз данных, используемых таможенными органами и регулярно пополняемых в режиме on-line при реализации таможенного контроля товаров и транспортных средств, перемещаемых через таможенную границу ежедневно. Всё это усложняется тем, что таможенные органы не ограничены каким-либо регионом РФ, а располагаются на всей территории России, а также имеют представительства за её границей, в связи с чем, используемая Единая автоматизированная информационная система таможенных органов (ЕАИС ТО) РФ, объединенная посредством ВИТС ФТС России применяется в формате 24/7, так как работа таможни не останавливается ни в ночное, ни в дневное время.

Кроме того, повсеместное использование в таможенных органах РФ продуктов Microsoft Office заставляет присмотреться к проектам перехода на российское программное обеспечение, выполняющее аналогичные функции и определение наиболее рациональных вариантов с учетом переформатирования, в том числе, ведения внутреннего документооборота и необходимости переобучения персонала работе на новых системах с минимальными затратами.

Отечественные аналоги Microsoft Office необходимо выбирать по принципу наибольшей функциональной схожести со средствами Microsoft Word, Excel, PowerPoint, Access, Outlook для решения полного функционала задач, возложенных на должностных лиц таможенных органов при их использовании и минимуме затрат на переориентацию сотрудников таможни при применении новых программных продуктов офисного типа, а также из совместимости с документами, полученными посредством Microsoft Office, и с операционными системами отечественных производителей, на которые будут переведены все рабочие места в ЕАИС ТО РФ, например, Astra Linux.

Широта применения СУБД Oracle при ведении БД в таможенных органах РФ требует перехода к СУБД отечественных производства, совместимых с Astra Linux, и поддерживающих функционал, необходимый для оперативной обработки больших объемов данных, измеряемых петабайтами информации. Всё вышеперечисленное подразумевает не только архивное хранение таможенной информации, но и её обработку, в том числе, в режиме on-line, различными автоматизированными, аналитическими, информационными, системами, комплексами программных средств и т. п.

В заключение отметим, что внедрение российского программного и аппаратного обеспечения, удовлетворяющего основным требованиям по информационной безопасности, отказоустойчивости, производительности и скорости обработки информации, возможности осуществления архивирования и оптимизации хранимой информации, а также осуществления качественного анализа больших объемов данных, обеспечит как эффективную работу таможенных органов, так и в целом, экономическую безопасность государства.

Информация о конфликте интересов

Мы, авторы данной статьи, со всей ответственностью заявляем о частичном и полном отсутствии фактического или потенциального конфликта интересов с какой бы то ни было третьей стороной, который может возникнуть вследствие публикации данной статьи.

ЛИТЕРАТУРА

1. Цифровая повестка ЕАЭС. URL: https://digital.eaeunion.org/upload/medialibrary/988/заявление %20о %20цифровой %20повестке %20ЕАЭС %20копия_пподписанное.pdf (дата обращения: 18.06.2024).

2. Значение деятельности таможенных органов в реализации таможенной политики Российской Федерации в современных условиях :

монография / под редакцией И. Т. Насретдинова. — Москва : Русайнс, 2015. — 140 с.

3. Об утверждении Методических рекомендаций по обеспечению необходимого уровня безопасности в сфере информационно-коммуникационных технологий государственных корпораций, компаний с государственным участием, а также их дочерних организаций и зависимых обществ : приказ Министерства цифрового развития, связи и массовых коммуникаций России от 10.03.2022 г. № 186. — URL: https://digital.gov.ru/ru/documents/8173/ (дата обращения: 18.06.2024).

4. О дополнительных мерах по обеспечению информационной безопасности Российской Федерации : указ Президента Российской Федерации от 01.05.2022 г. № 250. — URL: http://www.kremlin.ru/acts/bank/47796 (дата обращения: 18.06.2024).

5. Официальный сайт Президента РФ. — URL: http://www.kremlin.ru (дата обращения: 18.06.2024).

6. Об утверждении типового положения о заместителе руководителя органа (организации), ответственном за обеспечение информационной безопасности в органе (организации), и типового положения о структурном подразделении в органе (организации), обеспечивающем информационную безопасность органа (организации) : постановление Правительства Российской Федерации от 15.07.2022 г. № 1272. — URL: http://publication.pravo.gov.ru/Document/View/0001202207190035 (дата обращения: 18.05.2024).

7. Об утверждении Концепции формирования и развития культуры информационной безопасности граждан Российской Федерации : распоряжение Правительства РФ от 22.12.2022 г. № 4088-р. — URL: https://www.consultant.ru/document/cons_doc_LAW_435331/ (дата обращения: 18.06.2024).

8. Об утверждении Основ государственной политики Российской Федерации в области международной информационной безопасности : указ Президента РФ от 12.04.2021 № 213. — URL: https://www.consultant.ru/document/cons_doc_LAW_381999/ (дата обращения: 20.05.2024).

9. Официальный сайт Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации. — URL: digital.gov.ru/ru/documents/7342 (дата обращения: 18.06.2024).

10. Официальный сайт ФТС России. — URL: https://customs.gov.ru (дата обращения: 18.06.2024).

11. *Литова А.* Хакеры обрушили электронную систему ФТС / А. Литова, К. Потаева // Ведомости. — URL: https: // www.vedomosti.ru/business/articles/2023/04/11/970397-hakeri-obrushili-elektronnuyu-sistemu-fts (дата обращения: 20.05.2024).

12. *Ионина М. В.* Анализ подходов к обеспечению информационной безопасности компании / М. В. Ионина // Бюллетень инновационных технологий. — 2024. — Т. 8. № 1 (29). — С. 48—53. — URL: https://bitjournal.ru/index.php/BIT/article/view/352/552 (дата обращения: 10.05.2024).

13. О проведении эксперимента по созданию, переводу и развитию государственных информационных систем и их компонентов на единой цифровой платформе Российской Федерации «ГосТех» : постановление Правительством РФ от 12.10.2020 г. № 1674. — URL: https://www.consultant.ru/document/ cons_doc_LAW_365168/ (дата обращения: 18.05.2024).

14. Об утверждении Положения о единой цифровой платформе Российской Федерации «ГосТех», о внесении изменений в постановление Правительства Российской Федерации от 6 июля 2015 г. № 676 и признании утратившим силу пункта 6 изменений, которые вносятся в требования к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем и дальнейшего хранения содержащейся в их базах данных информации, утвержденных постановлением Правительства Российской Федерации от 11 мая 2017 г. № 555 : постановление Правительства РФ от 16 декабря 2022 г. № 2338. — URL: https://www.garant.ru/products/ipo/prime/doc/405880325/ (дата обращения: 18.06.2024).

15. Международный форум «Технология и безопасность». — URL: https: //www.tbforum.ru/hubfs/Digital/SS/SS_ADAPT/TBF24_14-02-24_Бондаренко.pdf?hsLang=ru (дата обращения: 18.06.2024).

16. *Минакова И. В.* Государственное управление внешнеторговой деятельностью на основе развития институтов таможенного администрирования : монография / И. В. Минакова, Н. Е. Деркач, О. И. Солодухина, С. А. Старых. — Курск : ЗАО Университетская книга, 2024. — 103 с.

17. Официальный сайт АНО «ЦКИТ». — URL: ru-ikt.ru (дата обращения: 19.05.2024).

18. Результаты мониторинга закупок программного обеспечения для обеспечения государственных и муниципальных нужд по состоянию на 01.01.2023 АНО «ЦКИТ». — URL: https://old.ru-ikt.ru/upload/iblock/707/Отчет %20о %20закупках %20ПО %202022 %20фин.pdf (дата обращения: 18.05.2024).

19. Каталог совместимости российского программного обеспечения (АРПП «Отечественный софт» АНО «ЦКИТ»). — URL: https://catalog.

arppsoft.ru/replacement_list (дата обращения: 18.06.2024).

20. Российский интернет-портал аналитического агентства TAdviser «Государство. Бизнес. Технологии». — URL: https://www.tadviser.ru/ (дата обращения: 18.05.2024).

21. Интернет-портал аналитического агентства «TADVAISER». — URL: www.tadviser.ru/index.php// (дата обращения: 19.05.2024).

22. Интернет-портал аналитического агентства «TADVAISER». — URL: https://www.tadviser.ru/index.php/ Статья:Информационная_безопасность_в_компании (дата обращения: 20.05.2024).

23. Интернет-портал по информационной безопасности в сети. — URL: https://safe-surf.ru/specialists/article/5303/683297/ (дата обращения:20.06.2024).

LITERATURE

1. The Digital Agenda of the EAEU. — URL: https://digital.eaeunion.org/upload/medialibrary/988/заявление %20о %20цифровой %20повестке %20EAES %20copy_appointed.pdf (date of access: 06/18/2024).

2. The importance of the activities of customs authorities in the implementation of the customs policy of the Russian Federation in modern conditions : monograph / edited by I. T. Nasretdinov. — Moscow : Rusains, 2015. — 140 p.

3. On approval of Methodological recommendations on ensuring the necessary level of security in the field of information and communication technologies of state corporations, companies with state participation, as well as their subsidiaries and Dependent companies : Order of the Ministry of Digital Development, Communications and Mass Media of Russia dated 03/10/2022 № 186. — URL: https://digital.gov.ru/ru/documents/8173 / (date of application: 06/18/2024).

4. On additional measures to ensure information security of the Russian Federation : Decree of the President of the Russian Federation dated 05/01/2022 No. 250. — URL: http://www.kremlin.ru/acts/bank/47796 (date of application: 06/18/2024).

5. The official website of the President of the Russian Federation. — URL: http://www.kremlin.ru (date of application: 06/18/2024).

6. On approval of the model regulation on the deputy head of the body (organization) responsible for ensuring information security in the body (organization), and the model regulation on the structural unit in the body (organization) ensuring information security of the body (organization) : Resolution of the Government of the Russian Federation № 1272 dated 07/15/2022. — URL: http://publication.pravo.gov.ru/Document/View/0001202207190035 (date of application: 05/18/2024).

7. On approval of the Concept of formation and development of the culture of information security of citizens of the Russian Federation : Decree of the Government of the Russian Federation dated 12/22/2022 № 4088-R. — URL: https://www.consultant.ru/document/cons_doc_LAW_435331 / (date of access: 06/18/2024).

8. On approval of the Fundamentals of the State Policy of the Russian Federation in the field of international information security : Decree of the President of the Russian Federation dated 04/12/2021 № 213. — URL: https://www.consultant.ru/document/cons_doc_LAW_381999 / (date of access: 05/20/2024).

9. Official website of the Ministry of Digital Development, Communications and Mass Media of the Russian Federation. — URL: digital.gov.ru/ru/documents/7342 (date of application: 06/18/2024).

10. Official website of the Federal Customs Service of Russia. — URL: https://customs.gov.ru (date of application: 06/18/2024).

11. *Litova A.* Hackers brought down the electronic system of the Federal Customs Service / A. Litova, K. Potaeva // Vedomosti. — URL: https://www.vedomosti.ru/business/articles/2023/04/11/970397-hakeri-obrushili-elektronnuyu-sistemu-fts (date of application: 05/20/2024).

12. *Ionina M. V.* Analysis of approaches to ensuring information security of the company / M. V. Ionina // Bulletin of innovative technologies. — 2024. — Vol. 8. No. 1 (29). — Pp. 48—53. — URL: https://bitjournal.ru/index.php/BIT/article/view/352/552 (date of application: 05/10/2024).

13. On conducting an experiment on the creation, translation and development of state information systems and their components on the unified digital platform of the Russian Federation «Gostech» : Decree of the Government of the Russian Federation dated 12.10.2020 № 1674. — URL: https://www.consultant.ru/document / cons_doc_LAW_365168/ (accessed: 05/18/2024).

14. On approval of the Regulations on the unified Digital Platform of the Russian Federation «GOSTECH», on Amendments to the Decree of the Government of the Russian Federation № 676 dated July 6, 2015 and invalidation of paragraph 6 of the amendments that are made to the requirements for the procedure for the creation, development, commissioning, operation and decommissioning of state information systems and further storage of information contained in their databases, approved by Decree of the Government of the Russian Federation dated May 11, 2017 № 555 : Decree of the Government of the Russian Federation dated December 16, 2022. № 2338. —

URL: https://www.garant.ru/products/ipo/prime/doc/405880325 / (date of access: 06/18/2024).

15. International Forum «Technology and Security». — URL: https://www.tbforum.ru/hubfs/Digital/SS/SS_ADAPT/TBF24_14-02-24_Бондаренко.pdf?hsLang=ru (date of reference: 06/18/2024).

16. *Minakova I. V.* State management of foreign trade activities based on the development of customs administration institutions : monograph / I. V. Minakova, N. E. Derkach, O. I. Solodukhina, S. A. Starykh. — Kursk : ZAO Universitetskaya kniga, 2024. — 103 p.

17. Official website of ANO «CCIT». — URL: ru-ikt.ru (date of access: 05/19/2024).

18. The results of monitoring the procurement of software for state and municipal needs as of 01.01.2023 ANO «CCIT». — URL: https://old.ru-ikt.ru/upload/iblock/707/Отчет %20о %20закупках %20ПО %202022 %20фин.pdf (date of reference: 05/18/2024).

19. Catalog of compatibility of Russian software (ARPP «Domestic software» ANO «CCIT»). — URL: https://catalog.arppsoft.ru/replacement_list (date of appeal: 06/18/2024).

20. The Russian Internet portal of the analytical agency TAdviser «The State. Business. Technology». — URL: // https://www.tadviser.ru / (date of access: 05/18/2024).

21. The Internet portal of the analytical agency «TADVAISER». — URL: www.tadviser.ru/index.php//Article: Large-scale import substitution projects (accessed: 05/19/2024).

22. The Internet portal of the analytical agency «TADVAISER». — URL: https://www.tadviser.ru/index.php / Article:Information security of the Company (date of application: 05/20/2024).

23. Internet portal for information security on the web. — URL: https://safe-surf.ru/specialists/article/5303/683297 / (date of request:06/20/2024).

УДК 338.242

ЦИФРОВАЯ ТОРГОВЛЯ КАК НЕОБХОДИМЫЙ ИННОВАЦИОННЫЙ ИНСТРУМЕНТ УПРАВЛЕНИЯ ТРАНСФОРМАЦИЕЙ ЭКОНОМИКИ РЕГИОНА

Коды JEL: O31, O27

Обухова А. С., *кандидат экономических наук, доцент, доцент кафедры финансов и кредита, Юго-Западный государственный университет, г Курск, Россия*
E-mail: obuhova_anna@inbox.ru; SPIN-код: 4085-8495

Барков И. М., *аспирант кафедры финансов и кредита, Юго-Западный государственный университет, г Курск, Россия*
E-mail: tracer9084@yandex.ru; SPIN-код: отсутствует

Ершова И. Г., *доктор экономических наук, профессор, профессор кафедры финансов и кредита, Юго-Западный государственный университет, г Курск, Россия*
E-mail: ershovairgen@yandex.ru; SPIN-код: 1024-2161

Поступила в редакцию 07.06.2024. Принята к публикации 28.06.2024

Аннотация

Актуальность темы. *Цифровые технологии завоевывают все области мировой экономики, включая международную торговлю. Все больше юридических и физических лиц предпочитают совершать покупки через цифровые платформы, что приводит к переходу многих услуг на онлайн-формат. Сегодня онлайн-платформы играют ключевую роль в сопоставлении спроса и предложения, упрощая сделки между всеми участниками рынка. Цифровая торговля переосмысливает традиционные процессы, включая платежи, электронный документооборот и электронную торговлю. Она также открывает новые перспективы, такие как внедрение искусственного интеллекта и цифровых решений в различные сферы торговли. Однако стоит учитывать, что развитие цифровой торговли несет как потенциальные выгоды, так и определенные риски для экономики. Для стабильного развития рынка цифровых товаров, цифровизации документооборота в B2B- и B2C-сегментах, разрешения торговых споров в электронном формате и использования искусственного интеллекта важно определить основные правила функционирования цифровой торговли в рамках ЕАЭС. Для поддержки развития цифровых технологий в Евразийском экономическом союзе могут*