3. *ОК 001–2021* (ИСО МКС). Общероссийский классификатор стандартов : издание официальное : введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 19 ноября 2021 г. № 1506-ст : дата введения 2022-01-01 / разработан ФГБУ «РСТ». – Текст : электронный // Техэксперт : [сайт]. – URL: https://docs.cntd.ru/document/727092529.

4. *Казанцева, Н. К.* Стандартизация в эпоху информационно-цифровой революции: взгляд провинции / Н. К. Казанцева, Т. В. Казанцева, Г. А. Ткачук // Стандарты и качество. – 2020. – № 2. – С. 30–34.

5. *Казанцева, Т. В.* Разработка подхода для цифровизации стандартов на метизную продукцию / Т. В. Казанцева, Н. К. Казанцева, М. А. Полякова // Международная научно-практическая конференции им. Д. И. Менделеева, посвященная 90-летию профессора Р. З. Магарила : материалы конференции, Тюмень, 25–27 ноября 2021 г. – Тюмень : Тюменский индустриальный университет, 2022. – С. 219–220.

6. *Федеральное агентство* по техническому регулированию и метрологии : официальный сайт. – Москва. – URL: http://www.standard.gost.ru. – Текст : электронный.

УДК 004.5 + 339.9.01

И. Д. Полежаев[1], Д. В. Полежаев[2], А. Д. Полежаева[3]

I. D. Polezhaev, D. V. Polezhaev, A. D. Polezhaeva

[1]ФГБОУ ВО «Московский институт радиоэлектроники и автоматизации – Российский технологический университет», Москва
[2]ГАУ ДПО «Волгоградская государственная академия последипломного образования», Волгоград
[3]ФГБОУ ВО «Всероссийская академия внешней торговли Минэкономразвития Российской Федерации», Москва

MIREA – Russian Technological University, Moscow
Volgograd State Academy of Postgraduate Education, Volgograd
Russian Foreign Trade Academy Ministry of economic development of the Russian Federation, Moscow

polezh@mail.ru

ВОПРОСЫ ЗАЩИТЫ ИНФОРМАЦИИ ВНЕШНЕТОРГОВОЙ ОРГАНИЗАЦИИ В УСЛОВИЯХ ЦИФРОВОЙ ЭКОНОМИКИ: НОРМАТИВНО-ПРАВОВОЙ АСПЕКТ

ISSUES OF PROTECTING INFORMATION OF A FOREIGN TRADE ORGANIZATION IN A DIGITAL ECONOMY: A REGULATORY AND LEGAL ASPECT

Аннотация. *В статье актуализируются социально-экономические и внутренне- и внешнеполитические аспекты обеспечения информационной безопасности внешнеторгового предприятия. Выделяются структурно-содержательные вопросы осуществления процессов экспортно-импортных операций в сфере высокотехнологичного оборудования.*

Анализируется в контексте темы исследования «Стратегия национальной безопасности Российской Федерации» как научно-методологическая и нормативно-правовая основа деятельности предприятия.

Abstract. *The article updates the socio-economic and domestic and foreign policy aspects of ensuring the information security of a foreign trade enterprise. Structural and substantive issues of the implementation of the processes of export-import operations in the field of high-tech equipment are highlighted. It is analyzed in the context of the theme of the research «National Security Strategy of the Russian Federation» as a scientific, methodological and legal basis for the activities of the enterprise.*

Ключевые слова: *информационная безопасность; внешнеэкономическая деятельность; внешнеторговое предприятие; экспортно-импортные операции; цифровая экономика.*

Keywords: *information security; foreign economic activity; foreign trade enterprise; export-import operations; digital economy.*

Вопросы информационной безопасности коммерческой и иной деятельности становятся все более актуальными в современных условиях, когда информационное обеспечение экономических процессов (сделок, соглашений, бизнес-проектов и др.), в том числе на уровне межгосударственных контрактов, становится неотъемлемо необходимым в повседневной работе предприятий, специализирующихся на осуществлении экспортно-импортных операций.

Изменения в осуществлении порядка и содержания торгово-экономических сделок, а также нормативно-правового / формального фиксирования итогового продукта / результата внешнеэкономической деятельности необходимо учитывается сегодня при оформлении актуальных, взаимно востребованных внешнеторговых контрактов и соглашений.

При этом следует учитывать, что информационное сопровождение, в том числе информационная защита / контроль сделки, проводится:

- во-первых, каждой стороной соглашения в отдельности, с учетом собственных интересов, с опорой на собственные информационно-компьютерные и финансово-экономические ресурсы с использованием доступных пространств их осуществления;
- во-вторых, с учетом внешних условий, устойчивых ритуалов, правил и норм, в том числе юридически фиксированных обязательств, закрепляющих определенного рода зависимость субъектов торгово-экономической деятельности, и привычно проявляющихся в ходе повседневной работы;
- в-третьих, в соответствии с изменяющимися (в том числе на уровне «форс-мажора») социально и внешнеполитическими условиями, возникающими или нарастающими явлениями и тенденциями их динамики, новыми субъектами внешнеэкономической деятельности и иными акторами, составляющими вместе «большое поле» торгово-экономического взаимодействия партнеров по экспортно-импортным операциям.

Нормативно-правовые основания информационно-аналитической деятельности в отношении организации, выступающей одним из основных субъектов, активных партнеров реализации внешнеторговой операции того или иного рода, необходимо опираются сегодня – в качестве в качестве наиболее общей нормативно-правовой базы на такой актуальный государственный документ, как «Стратегия национальной безопасности Российской Федерации» [4]. В Стратегии сформулированы важнейшие фундаментальные ценности и принципы современного российского общества и государства, существенные также для каждого отдельного человека – гражданина страны.

С одной стороны, данный документ, как продукт долгосрочного научного анализа осуществляется с учетом самых различных критериев, факторов, природно-климатических, социально-политических явлений и иных структурных компонентов общей картины мира субъекта – как многоуровневого и структурно сложного, так и малого – индивида [5, с. 50–55], в личностном пространстве которого определенным образом отражаются все течения и взаимопересекающиеся воздействия большого актора социально-государственной жизни. С другой, «Стратегия национальной безопасности» выступает, как основополагающий документ, регулирующий правила реализации социального, в том числе социально-экономического, взаимообмена и особенности взаимоотношения субъектов деятельности – как в целом, так и в сфере внешнеэкономических отношений.

Технологические вопросы защиты информации от несанкционированного внешнего воздействия опираются сегодня преимущественно на использование специальных информационно-технических компьютерных приспособлений, выступающих, например, в качестве наложенных средств защиты информации от стороннего доступа [8, с. 434–440]. Частичная или полная реализация такого рода информационных угроз в торгово-экономической практике может вызвать вполне серьезные негативные последствия для политики и бизнеса: и как общий репутационный ущерб фирмы-экспортера, и как крупные финансовые потери, а также остановка бизнес-процессов.

Следует помнить о вполне реальной опасности утечки информации так называемого «ограниченного доступа». Это особо важно, если речь идет не просто о личных данных субъекта внешнеэкономической деятельности, а сохранении государственной тайны или специальных данных, обеспечение сохранности которых регулируется на государственном уровне. Такого рода информация, в т.ч. экономического плана находится под контролем Федеральной службы безопасности России, а также Федеральной службы по техническому и экспортному контролю Российской Федерации.

Те или иные нарушения в области технической защиты специальной информации в области лицензирования, экспортного контроля, кадрового обеспечения и др. ведет к определенным воздействиям со стороны отвечающих за данный блок информации организаций и учреждений. Штрафные санкции могут в значительной степени «скорректировать» бизнес-процессы того или иного предприятия вплоть до полной остановки его уставной деятельности. Поэтому постоянное отслеживание значимого в плане безопасности информационного потока – задача не только внешних контролеров, но и собственно субъекта экономической деятельности, заинтересованного в ее продолжении и продуктивном развитии.

Для этого применяется мониторинг информационной системы внешнеторгового предприятия – необходимая предварительная работа по отслеживанию деструктивных событий различного вида. В настоящее время, по открытым данным на август 2021 г., используются около пятидесяти инструментов для такого мониторинга работы компьютерных система, отслеживающих в том числе особенности работы высокотехнологичного промышленного оборудования. Впрочем, система оперативного ограничения вредоносного воздействия извне на работу комплексов аппаратного программного обеспечения машин и оборудования развивается, прирастая, в свою очередь, – в зависимости от особенностей и новаций атак киберпреступников – средствами противодействия, в отношении как отдельных инцидентов, связанных с временной остановкой технологического, в том числе операционно-логистического процесса на внешнеторговом предприятии, так и с нарушением целостности общей организационно-управленческой среды фирмы и целенаправленного причинения ей прямого ущерба.

Для противодействия жестко направленному извне деструктивному воздействию на структуру, процесс и общий результат (продукт) внешнеторгового предприятия, его IT-инфраструктура должна быть оснащена надлежащими механизмами резервирования и аварийного восстановления данных. Если речь здесь идет об уже свершившемся акте кибер-атаки и т. п., и необходимости избежать общего финансово-экономического обрушения объекта, то следует, например, хранить носители резервных копий отдельно от резервной системы с защитой от несанкционированного доступа или неправомерного ее использовании – вплоть до восстановления резервной копии в новой системе или виртуальной машине.

Впрочем, если речь идет уже о предотвращении попытки несанкционированного доступа к конфиденциальным данным той или иной внешнеторго-

вой компании, то ряд общих для всех предварительных организационных мероприятий по организации информационной безопасности является гораздо более широким.

Полагаем важным отметить, что в последние годы мировой тенденцией стало то, что «мишенью» для программ-вымогателей являются не только крупные корпорации, но и компании из сегмента среднего и малого бизнеса, в том числе и в России. Количество атак на организации на территории РФ в 2021 г. увеличилось более чем на 200 %. Размер запрашиваемого у российских компаний выкупа, как правило, зависит от величины организации. Средний выплаченный выкуп в 2021 г. составил порядка три миллиона рублей. Среднее время простоя атакованной компании составляет 18 суток [7, с. 563–570]. Эти показатели включают в себя и иностранные кампании или их подразделения, которые ведут экономическую деятельность на территории нашей страны.

Видится важным здесь кратко охарактеризовать некоторые особенности внешнеэкономической деятельности современных совместных торговых предприятий, организаций и объединений, специализирующихся на осуществлении экспортно-импортных операций, реализующих те или иные механизмы внешнеторговой логистики. Это важно особенно в отношении деятельности предприятий, выступающих своеобразными «трансляторами» современных информационно насыщенных, наукоемких высокотехнологичных товаров.

Организационно-управленческая структура любого предприятия, активно ведущего направленную внешнеэкономическую деятельность в области высоких технологий, интересна по многим показателям, на некоторых из которых мы останавливались ранее [2, с. 37–44]. Но в первую очередь она важна, с точки зрения обеспечения экспортных каналов внешнеторговой фирмы, поскольку связана с правовыми, экономически, управленческими, кадровыми и другими положительно выстроенными из наличных, или вновь созданными условиями и ресурсами.

Важнейшей качественной характеристикой внешнеторговой фирмы с точки зрения организации логистики поставок продукции предприятия является география расположения предприятий корпорации. Однако не уйти и от понимания того, что в соответствии с пространственно-географическим протяжением компании выстроена и информационно-экономическая цепочка взаимодействия на всех ее предприятиях, в том числе через призму феномена социальной информации и социальной направленности деятельности индивидуально-личностного и социально-группового планов, что важно с точки зрения международно-экономического – экспортно-импортного измерения процессов. Это позволяет, с одной стороны, оптимизировать организационно-управ-

ленческие связи предприятия, преодолевая возникающие трудности логистическим средствами, в том числе внешнелогистической деятельности; с другой – делает «растянутую» структуру более уязвимой. Таких аспектов проблемы множество; но в данном случае существенно важным представляется поиск юридически значимых оснований реализации действий по защите коммерчески, политически и в иных смыслах значимой информации.

Полагаем необходимым повторить, что важнейшим нормативно-правовым аспектом проблемы осуществления информационно-технологической безопасности деятельности внешнеторгового предприятия выступает сегодня «Стратегия национальной безопасности Российской Федерации», структурно-содержательные элементы которой являются необходимыми ориентирами общей государственно-национальной политики современной России в отношении актуальных вопросов национального российского самоосуществления, самосознания и самореализации в условиях «диалога культур» – взаимодействия заинтересованных субъектов, авторов социально-экономической жизни в пространстве наличной культуры.

Вопросы обеспечения информационной безопасности согласно «Стратегии национальной безопасности» в общем и целом ориентированы на практическое применение предложенных регуляторов – как в рамках осуществления деятельности малых предприятий, фирм и т. п., так и крупных торгово-промышленных комплексов, объединений, корпораций. Однако они несут в себе достаточно серьезное политическое содержание, поскольку инновационные, научно-технические и научно-технологические достижения входят в число ключевых индикаторов конкурентоспособности любой страны, в том числе нашей России, в условиях глобального информационного мира.

Формирование безопасного, то есть – здесь – защищенного от деструктивного внешнего воздействия, пространства признается в Стратегии в качестве одного из важнейших стратегических национальных приоритетов нашего государства, наряду со «сбережением народа России и развитием человеческого потенциала», «государственной и общественной безопасностью», «защитой традиционных российских духовно-нравственных ценностей, культуры и исторической памяти» и других [4].

Информационная сфера жизнедеятельности общества и человека – это пространство, в котором может быть осуществлено манипулирование сознанием и поведением человека, что при отсутствии необходимого контроля опасно, как в политическом, национальном или религиозном отношении (это, как известно, наиболее устойчивые направления разрушительного влияния на сознание современной молодежи экстремистски направленных психологиче-

ских установок [6, с. 20–31]), так и в плане финансово-экономического измерения продуктивности торгово-экономической и торгово-промышленной деятельности инновационного внешнеторгового предприятия.

Видится необходимым помнить о вполне обоснованной опасности использования информационно-коммуникационных технологий в преступных целях, а потому важно работать в том числе над сохранением / или формированием установок позитивного экономического правосознания [1, с. 168–176], а потому проблема информационной безопасности экономической деятельности предстает в совершенно особом ключе. Особенно важно это учитывать, если человек обращает поведенческие векторы экономического правосознания на внешнеэкономическую деятельность, где правовые стороны осуществления экспортно-импортных операций достаточно сильно отличаются в зависимости от местоположения международного рыночного пространства.

Увеличение количества компьютерных атак на российские информационные ресурсы – опасность, которая касается, как государственно-политических компьютерно-коммуникационных систем, так и торгово-экономических пространств, заполненных фирмами и компаниями (в качестве примера мы однажды рассматривали японскую корпорацию ООО «Ямазаки Мазак») [3, с. 84–91], которая в настоящее время сильно сократила (пока еще не свернув окончательно) свою деятельность в России, попав в струю поддержки наращивания в отношении Российской Федерации незаконных экономических санкций, вводимых странами Запада и теми, кто находится под их влиянием с целью подрыва экономической устойчивости нашей страны. А потому «переструктуризация» внешней и внутренней экономики России в настоящее время выступает главной задачей, которую невозможно решить без должного информационно-компьютерного сопровождения, в том числе с точки зрения обеспечения информационной безопасности, основанной на применении инновационных практико-ориентированных технологий защиты [9, с. 84–89].

Сегодня распространение недостоверной финансово-экономической информации, в первую очередь, транснациональными корпорациями, опирается на их настойчивое стремление к закреплению собственного монопольного положения на внешнем рынке и в глобальной информационно-коммуникационной системе – сети интернет, а также к функциональному контролю всех информационных ресурсов (средствами цензуры, блокировки неангажированных интернет-платформ).

Понятно, что анонимность как критерий реализации информационно-коммуникативных действий, целенаправленных в разрушительном политическом, экономическом, культурно-психологическом и ином отношении, облег-

чает совершение преступных экономических действий, что необходимо учитывается специалистами в области обеспечения информационной безопасности деятельности торгово-промышленных производственных предприятий, в том числе специализирующихся на вопросах оформления и сопровождения экспортно-импортных операций с высокотехнологичными наукоемкими товарами и технологиями.

Многоуровневая задача, направленная на обеспечение информационной безопасности в целом, может быть вполне убедительно представлена в рамках повышения защищенности информационной структуры субъекта внешнеэкономической деятельности, может быть представлена в виде схемы (рис. 1).

Рис. 1. Схема многоуровневой задачи

Такого рода системная и многоуровневая задача, аспектно представленная в схеме, необходимо опирается на определенного рода (с разумными ограничениями) информационную открытость общества и государства, направленную как «вовне» – на партнеров и оппонентов, так и «внутрь» страны. Последнее особо важно для поиска общих устойчивых точек опоры ментального, духовно-идеологического плана, без которых технологические вопросы информационного обеспечения безопасности останутся лишь прикладными, функционал которых может быть применим как в позитивном, содержательном, так и в деструктивном ключе.

Заключая наши рассуждения о проблеме обеспечения информационной безопасности внешнеэкономических предприятий в условиях цифровой эко-

номики, следует отметить, что именно в этом направлении следует искать перспективы развития высокотехнологичных сфер экономической деятельности современной России – нано-технологий, робототехники, биологической и генной инженерии, квантовых технологий и технологий искусственного интеллекта, технологий обработки массивного объема данных и многого другого.

Именно эти направления видятся нам актуальными, как в научном плане, так и в практическом отношении – с точки зрения решения известных и возможных вопросов обеспечения информационной безопасности внешнеторгового предприятия в условиях международной цифровой экономики и глобального информационно-коммуникационного пространства. Но рассматривать их применительно к практике необходимо с учетом того, что единство социально-экономических механизмов и пространств реализации внешнеэкономической деятельности обеспечивается не только общими критериями и характеристиками субъектов внешнеэкономической деятельности, но также особенностями их повседневного проявления и единичными актами, имеющими ментальную природу; то есть важно помнить об учете национально-государственной, в том числе нормативно-правовой специфики при решении тех или проблем и вопросов защиты информации в условиях цифровой экономики.

Список литературы

1. *Ануфриева, Е. В.* Экономическое правосознание и его отражение в современном русском менталитете / Е. В. Ануфриева, Д. В. Полежаев // Бизнес. Образование. Право. Вестник Волгоградского института бизнеса. – 2010. – № 2 (12). – С. 168–176.

2. *Кархова, И. Ю.* Вопросы организации экспортных поставок высокотехнологичного оборудования (Социально-экономические аспекты внешнеторговой логистики) / И. Ю. Кархова, А. Д. Полежаева // Primo Aspectu. – 2021. – № 3 (47). – С. 37–44.

3. *Кархова, И. Ю.* Внешнеторговая логистика предприятия: некоторые аспекты регулирования экспортных поставок высокотехнологичного оборудования / И. Ю. Кархова, А. Д. Полежаева // Техническое регулирование в едином экономическом пространстве : сборник статей VIII Всероссийской научно-практической конференции с международным участием, Екатеринбург, 19 мая 2021 г. – Екатеринбург : РГППУ, 2021. – С. 84–91.

4. *О Стратегии* национальной безопасности Российской Федерации : Указ Президента Российской Федерации № 400 от 02.07.2021 г. – Текст : электронный. – URL: http://www.kremlin.ru/acts/bank/47046/page/5.

5. *Полежаев, Д. В.* Проблема формирования картины мира личности / Д. В. Полежаев // Известия Волгоградского государственного педагогического университета. – 2009. – № 8 (42). – С. 50–55.

6. *Полежаев, Д. В.* Социология молодежного экстремизма: каузальный анализ взаимодействия современных субкультур / Д. В. Полежаев // Primo Aspectu. – 2018. – № 4 (36). – С. 20–31.

7. *Полежаев, И. Д.* Информационная безопасность современного внешнеторгового предприятия: технологические возможности защиты от IT-вмешательства / И. Д. Полежаев, Д. В. Полежаев // Актуальные социально-экономические проблемы развития общества

в России и за рубежом : материалы III Всероссийской научно-практической конференции с международным участием, Волгоград, 26 ноября 2021 г. / Волгогр. ин-т бизнеса. – Волгоград; Саратов : Амирит, 2021. – С. 563–570.

8. *Полежаев, И. Д.* Наложенные средства защиты информации от несанкционированного доступа: современное состояние и перспективы совершенствования / И. Д. Полежаев, Д. В. Полежаев // Мультипликация кризисных сценариев в современном социуме и пути их преодоления : материалы Международной конференции, Ставрополь, 25 декабря 2020 г. – Ставрополь : АНО ВО СКСИ, 2020. – С. 434–440.

9. *Полежаев, И. Д.* Проблемы информационной безопасности в современном мире: практико-технологические аспекты защиты информации / И. Д. Полежаев, Д. В. Полежаев // Человек в современных социально-философских концепциях : материалы III Всероссийской научно-практической конференции, Елабуга, 26–27 ноября 2020 г. – Казань : Изд-во Казан. ун-та, 2020. – С. 84–89.

УДК 330.522

Д. П. Швецов

D. P. Shvetsov

ООО «Центр точного литья», Екатеринбург

Precision Casting Center, Ekaterinburg

shwedmail@gmail.ru

НОВЫЕ ГОРИЗОНТЫ ДЛЯ РОССИЙСКИХ ПРОИЗВОДИТЕЛЕЙ

NEW HORIZONS FOR RUSSIAN MANUFACTURERS

Аннотация. *В данной статье рассмотрен положительный опыт замены импортных расходных материалов на отечественные на примере литейного производства. Приведен анализ перспектив развития импортозамещения в разных направлениях.*

Abstract. *This article discusses the positive experience of replacing imported consumables with domestic ones using the foundry industry as an example. An analysis of the prospects for the development of import substitution in different directions is given.*

Ключевые слова: *импортозамещение; российский аналог; экономические санкции; литейное производство.*

Keywords: *import substitution; Russian analogue; economic sanctions; foundry.*

Сейчас как никогда актуален вопрос о российских аналогах и собственных разработок почти во всех сферах деятельности и жизни, от товаров и вещей общего пользования, до комплектующих и расходников для производств. Всем необходимо адаптироваться, искать альтернативные варианты или способы работы в условиях возникших ограничений. Всем этим обусловлена актуальность данной работы и дальнейшее изучение этих вопросов.