Федеральное государственное бюджетное учреждение науки
ЦЕНТРАЛЬНЫЙ ЭКОНОМИКО-МАТЕМАТИЧЕСКИЙ ИНСТИТУТ РАН
CENTRAL ECONOMICS AND MATHEMATICS INSTITUTE RAS

РОССИЙСКАЯ
АКАДЕМИЯ НАУК

RUSSIAN
ACADEMY OF SCIENCES

А.С. Славянов, Е.Ю. Хрусталев

МЕТОДОЛОГИЧЕСКИЕ ПОДХОДЫ К ФОРМИРОВАНИЮ ГОСУДАРСТВЕННОЙ ПОЛИТИКИ В СФЕРЕ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ

Монография

Москва
2022

УДК 338.22:339.97 **DOI:** 10.33276/978-5-8211-0808-1
ББК 65.050
С47

С47 **Славянов А.С., Хрусталев Е.Ю.** Методологические подходы к формированию государственной политики в сфере национальной безопасности [Текст]: монография. – М.: ЦЭМИ РАН, 2022. – 114 с. (Рус.)

В монографии проведен анализ наиболее серьезных внешних угроз, на основании которого разработаны принципы формирования стратегии защиты социально-экономической системы. Издание включает в себя две части: в первой исследуются вероятные угрозы суверенитету государства; во второй предложены подходы к организации системы безопасности. Данное исследование предназначено для работников научных организаций, министерств и ведомств, участвующих в планировании развития стратегических отраслей экономики, а также сотрудникам силовых ведомств, занятых в формировании системы национальной безопасности.

Ключевые слова: экономическое развитие, угрозы, риски, экономическая защита, торговые и финансовые ограничения; социально-экономическая система; информационная и технологическая безопасность
JEL: F51, F52, O25.

Slavyanov A.S., Khrustalev E.Yu. Methodological approaches to the formation of state policy in the field of national security [Text]: monograph. – Moscow: CEMI Russian Academy of Sciences, 2022. – 114 p. (Rus.)

The monograph analyzes the most serious external threats, on the basis of which the principles of forming a strategy for the protection of the socio-economic system are developed. The publication includes two parts: – the first examines possible threats to the sovereignty of the state; the second suggests approaches to the organization of the security system. This study is intended for employees of scientific organizations, ministries and departments involved in planning the development of strategic sectors of the economy, as well as employees of law enforcement agencies involved in the formation of the national security system.

Keywords: economic development, threats, risks, economic protection, trade and financial restrictions; socio-economic system; information and technological security.
JEL: F51, F52, O25.

Рецензенты: Б.А. Ерзнкян, д.э.н., профессор;
П.А. Дроговоз, д.э.н., профессор.

УДК 338.22:339.97
ББК 65.050

ISBN 978-5-8211-0808-1

© Текст. Славянов А.С., Хрусталев Е.Ю., 2022 г.
© ФГБУН Центральный экономико-математический институт РАН, 2022 г.

ОГЛАВЛЕНИЕ

Введение 4
Глава 1. Основные угрозы безопасности экономической системе 8
1.1. Обзор основных угроз 8
1.2. Вооруженные конфликты 9
1.3. Гибридные войны 11
1.4. Экономические войны 14
1.5. Технологические угрозы 18
1.6. Киберугрозы 30
1.7. Коррупция и нелегальное финансирование бизнеса 33
Глава 2. Подходы к построению системы безопасности экономической системы 35
2.1. Принципы формирования стратегии безопасности экономической системы 35
2.2. Подходы к планированию развития силового блока системы безопасности 40
2.3. Организация экономической защиты системы 58
2.4. Научные исследования и разработки как элемент защиты экономической системы 66
2.5. Система информационной безопасности 77
2.6. Методы повышения эффективности экономической защиты 94
2.7. Подходы к противодействию нелегальному финансированию бизнеса и коррупции 102
Заключение 106
Литература 108

ВВЕДЕНИЕ

В настоящий момент цивилизация, построенная на рыночных принципах, переживает глубокий кризис, вызванный не только последствиями пандемии, но и деградацией международных отношений на фоне общей нестабильности мировой финансовой системы. Стремясь компенсировать свои потери, глобальные финансовые корпорации прикладывают все усилия не для стабилизации рынков, а для обострения международной обстановки и перевода тлеющих различных региональных экономических и социально-политических конфликтов в фазу вооруженных столкновений. Данная стратегия позволяет решить две задачи: государство может отсрочить выполнение своих обязательств или вовсе списать задолженности, а корпорации могут получить дополнительное финансирование на производство вооружений, военной техники и амуниции.

Вместе с тем, такая политика, хотя и позволяет государству и корпорациям решить ряд задач, но существенно снижает барьеры на пути к глобальному вооруженному конфликту с применением ядерного оружия. В связи с тем, что к началу 2022 г. была практически разрушена система международной безопасности, основанная на договорах о ликвидации ракет средней и меньшей дальности, об ограничении систем противоракетной обороны, стратегических наступательных вооружений и других, вероятность применения оружия массового поражения существенно возросла.

Не вызывает сомнений и то обстоятельство, что вооруженные конфликты между экзистенциальными противниками могут привести к разрушению не только военной, но и гражданской инфраструктуре, что является неприемлемым для обеих сторон. В течение последнего десятилетия были созданы основанные на новых физических принципах уникальные вооружения, практически обесценивающие имеющийся у конфликтующих сторон весь наступательный и оборонительный потенциал.

Достижение цели в этих обстоятельствах возможно, на наш взгляд, двумя средствами:

- перенесение конфликта между двумя противниками на другую территорию и ведение военных действий с помощью ресурсов третьей страны, что уже неоднократно происходило и происходит в современной истории;
- использование невоенных методов или так называемой «мягкой силы».

Распад СССР и отторжение от России исторически связанных с ней территорий, ликвидация российских военных баз за рубежом, а также разрушение связей с союзными государствами, является тому примером. Ужесточение в течение короткого промежутка времени экономических санкций, информационные вбросы и

кибернетические атаки против стратегических предприятий, органов власти и общественных организаций, угрозы и реализация финансовой и торговой блокады, организация в непосредственной близости от границ беспорядков, социальных волнений и проведение масштабных военных учений, провокации в отношении российских организаций и граждан за рубежом, спонсирование террористических группировок, вступающих в прямые боестолкновения с нашими союзниками, говорит о том, что против России развернулась полномасштабная гибридная война.

После очередного расширения спектра санкционных ограничений в 2022 г. сложилась ситуация, которую уже можно считать объявлением экономической, а также информационной и культурной войны нашей стране. Для противодействия торговым и инвестиционным ограничениям руководство Российской Федерации еще в 2014–2015 гг. разработало комплекс отраслевых стратегий импортозамещения и локализации производства аналогов импортного оборудования и комплектующих на территории нашей страны. Каждая из отраслевых стратегий включает в свой состав ряд первоочередных мероприятий, направленных на поддержку финансового состояния и развитие производства замещаемых компонентов на предприятиях ведущих секторов российской экономики. Представляется очевидным, что для их выполнения предприятия должны иметь в своем распоряжении систему критериальных и результирующих показателей, необходимых для оценки эффективности их деятельности.

Для защиты национальных интересов Российской Федерации необходимо разработать новую государственную политику, адекватную современным условиям и основанную на противостоянии в экономической и военной сфере с использованием ресурсов третьих стран.

Исследование направлено на разработку методологии формирования государственной политики в сфере национальной безопасности в условиях усиливающегося внешнего экономического, информационного и политического давления на Россию. Решение данной проблемы имеет важное народнохозяйственное значение и носит фундаментальный характер.

Проблема обеспечения экономической безопасности была исследована отечественными учеными в разных аспектах. Наиболее значимыми можно признать работы Д.Е. Плисецкого [1], где был проведен анализ влияния иностранного капитала на финансовую устойчивость развивающихся государств, а также Н.Н. Кауровой [2], считающей неопределенность мировой финансовой системы и связанные с ней дисбалансы главной угрозой обществу.

Глубокий исторический анализ процессов глобализации и их влияния на безопасность государств проведен в работах Г.Г. Попова [3], В.Г. Ольшевского [4]

и Ю.В. Латова [5]. Анализу рисков и формированию резервов, как метода защиты, посвящена работа В. Батадеева [6]. В своей работе «Национальный суверенитет и экономическая безопасность в условиях применения экономических санкций» А.Е. Городецкий [7] предлагает активизировать программу импортазамещения, которая должна способствовать повышению уровня национальной безопасности в условиях санкционного давления на Россию.

Проблеме противодействия информационным провокациям и экстремистским движениям, возникающим на почве межнациональных отношений и этнокультурной самоидентификации, в том числе в социальных сетях посвящена работа Д.В. Перковой и А.Н. Худолеева [8]. Роль национальной идеи в формировании государственной политики безопасности выявлена в работе В.Н. Пасичника [9]. Достаточно много работ посвящено исследованию проблем продовольственной, топливной, кибернетической, информационной и других видов безопасности, анализируется их роль в формировании государственной политики. Общим проблемам формирования стратегии экономической безопасности посвящены работы В.К. Сенчагова [10] (наиболее значимая из которых «Новые угрозы экономической безопасности и защита национальных интересов России», в которых проводится анализ существующих и новых угроз. Интерес вызывает, разработанная В.К. Сенчаговым система показателей, позволяющая определить угрозы и вызовы социально-экономическому развитию страны, а также меры по защите национальных интересов России. Проблемам обеспечения экономической безопасности государства посвящены работы В.М. Безденежных [11] и В.И. Авдйского [12].

Важную и обширную научно-исследовательскую работу в области национальной безопасности выполняют ученые и специалисты Академии военных наук, Российской академии ракетных и артиллерийских наук, Академии проблем военной экономики и финансов, Центральных научно-исследовательских институтов Минобороны РФ, которые свои научные труды посвящают проблемам экономики военного строительства государства и военной реформы, становления и развития военно-экономической науки. Значительное внимание они уделяют анализу наиболее актуальных вопросов практики и теории невоенных войн, которые осуществляются в экономике, финансах, на информационном поле. Особо тщательно анализируются современные тенденции развития форм межгосударственного противоборства [13]. В статье В.Л. Гладышевского и Е.В. Горголы Е.В. [14] утверждается, что одной из наиболее опасных и результативных форм гибридной войны Запада против России, безусловно, является сетевая война, означающая заведомое установление полного и абсолютного контроля над всеми участниками актуальных или возможных боевых действий и тотальное манипулирование ими во всех ситуациях – как во время мира, так и войны.

Для решения задач обеспечения национальной безопасности России в современных условиях важно учитывать своевременность и действенность мер по организации эффективного противодействия сетевой агрессии, возможность задействовать в необходимый момент все потребные ресурсы и одновременно не дать противнику шансов подчинить их себе или каким-либо образом ограничить их использование. В соответствии с сетевой оборонительной стратегией должна быть сформирована совокупность таких комбинаций различных ресурсов и таких разных сетевых технологий, с которыми агрессор в нынешнем своем состоянии не справится. Сетевую войну можно выиграть только сетевыми средствами, адаптировав к собственным условиям и целям эффективные и стремительно развивающиеся технологии.

Главная методологическая проблема, на решение которой были направлены основные усилия С.Ф. Викулова С.Ф. [15], состоит в установлении содержания, роли и места сетевых финансовых и экономических войн в современной России. При этом достаточно корректно определяются роль и место военно-экономической науки как научной дисциплины среди научных дисциплин фундаментального и прикладного характера. Важным результатом этого исследователя представляется вывод о том, что для предотвращения необоснованности в принятии управленческих решений, влияющих на безопасность государства, военная экономика как наука и, соответственно, учение о ее перманентно меняющейся парадигме, должна развиваться опережающими темпами, поскольку она призвана устанавливать объективные закономерности и на этой основе вырабатывать способы воздействия на окружающий мир во всех аспектах.

Вместе с тем, не смотря на достаточно глубоко исследованные частные аспекты безопасности, в отечественной науке отсутствует единые методологические подходы к формированию политики в сфере национальной безопасности с учетом новых вызовов и угроз. Также до настоящего времени не выработан системный подход к организации эффективной защиты от угроз ведения прокси-войн и гибридных конфликтов в информационном пространстве, финансовой и внешнеэкономической сфере.

Поставленная в Послании Президента РФ задача реализации национальных проектов не может быть полностью выполнена, если не будет разработана система противодействия новым вызовам и угрозам со стороны ряда индустриально развитых государств в финансовой, информационной, социальной и экономической сферах. В связи с этим, приоритетной целью государственной политики должен стать системный подход к обеспечению безопасности социально-экономического развития России, сохранению ее суверенитета и укреплению позиций на мировой экономической и политической арене.

ГЛАВА 1.
ОСНОВНЫЕ УГРОЗЫ БЕЗОПАСНОСТИ ЭКОНОМИЧЕСКОЙ СИСТЕМЕ

1.1. Обзор основных угроз

Угрозы для социально-экономических систем могут представлять различные природно-климатические катаклизмы, космические катастрофы, эпидемии и конфликты между странами, этносами, религиозными или социальными группами. Можно заметить, что вероятность возникновения глобальных биологических, геологических, космических катастроф на данном историческом периоде представляется ничтожной и человечество не в состоянии им противостоять, в то время как риск разрушительного международного конфликта в настоящее время представляет реальную опасность для каждой экономической системы.

Наблюдения за ходом развития цивилизации дают основания предполагать, что государства не могут долго находиться в состоянии гармонии друг с другом и внешней средой. Истощение ресурсов, природные, социальные катаклизмы и другие факторы создают условия для различного рода конфликтов, которые носят в основном экономический характер, маскируемые правовой, религиозной, политической или иной вуалью. Проблемам конфликтологии посвящены труды отечественных и зарубежных ученых, которые разделяют конфликты на группы по различным признакам. Выделяются этнические и религиозные конфликты [16], международные и региональные [17], экономические [18], политические, ассиметричные конфликты [19] и др. В данном исследовании будем рассматривать конфликты как насильственные (горячие) и ненасильственные (холодные).

Исследователи в данной области справедливо полагают, что в условиях современного развития технологий, военные действия будут представлять собой серию точечных операций, целью которых будет лишение противника ресурсов, необходимых для сопротивление, а использование высокоточных средств дистанционного поражения снимет границу между фронтом и тылом. Боевые задачи будут выполнять высокотехнологичные мобильные соединения небольшой численности [20]. Наблюдения показывают, что вооруженные конфликты, имевшие место в разных точках планеты на рубеже XX–XXI вв., были спровоцированы ведущими мировыми или региональными державами, которые непосредственного участия в столкновениях не принимали. Цели достигались с помощью третьих сил, применение которых определяется специалистами, как прокси-война. Использование прок-

си-ресурса позволяет с одной стороны, снизить вероятность разрушительной ядерной войны, с другой – снижает финансовые затраты и политические риски в случае возможного поражения [21].

Серьезную опасность представляют собой использование сторонами различных ограничений в сфере торговли, инвестиций и трудовой миграции. Эти инструменты получили достаточно широкое распространение в послевоенный период и применяются в настоящее время. Последствия финансово-экономических санкций могут нанести гораздо более тяжелый ущерб государству, чем физические разрушения объектов инфраструктуры в результате боевых действий.

Серьезные угрозы формируются в сфере информационных технологий, которые используются практически во всех видах экономической деятельности, на всех уровнях управления, включая государственный аппарат, образование, СМИ. Кибератаки, информационные вбросы могут парализовать деятельность банковской и транспортной системы, отраслей промышленности, систему безопасности на федеральном и местном уровне. Информационные ресурсы являются важнейшим инструментом гибридной войны, которая может не только существенно затормозить развитие экономической системы, но и привести к ее частичному или полному разрушению.

В данной работе будут рассмотрены угрозы, имеющие высокую вероятность реализации и которые могут быть нивелированы посредством специальных мероприятий. К такого рода угрозам можно отнести вооруженный конфликт, финансово-экономические и торговые войны, технологические угрозы, гибридные войны, киберугрозы, а также коррупция и нелегальное финансирование бизнеса.

1.2. Вооруженные конфликты

История человечества была и остается историей войн. За последние пять с половиной тысячелетий произошло 14,5 тыс. войн. Погибло, умерло от эпидемий и голода более 3,6 млрд человек. При этом тенденция роста потерь заставляет внимательнее отнестись к изучению этого явления. Так, только в Европе потери в войнах (убитые и умершие от ран) составили: в XVII в. – 3,3 млн чел., в XVIII в. – 5,4, в XIX и начале XX в. (до Первой мировой войны) – 5,7 млн, в Первой мировой войне – свыше 9 млн, а во Второй мировой войне – свыше 50 млн человек. Политики и военные специалисты давали различные толкования понятия война. Например, в определении классиков марксизма-ленинизма под войной понималась организованная вооруженная борьба между государствами (группами государств), классами или нациями и народами. Современная классическая литература трактует

войну как вооруженный конфликт между политическими образованиями – государствами, племенами, политическими группами. Определение подчеркивает наличие конфликта сторон, проходящего в форме вооруженного противоборства, военных (боевых) действий между их вооруженными силами [22]. Большая советская энциклопедия вкладывает в определение войны дополнительные смыслы: «…Для достижения политических целей в войне используются вооруженные силы как главное и решающее средство, а также экономические, дипломатические, идеологические и другие средства борьбы» [23]. Следует подчеркнуть, что во всех приведенных формулировках подчеркивается мысль о том, что война предполагает наличие и использование средств вооруженной борьбы. В настоящее время получила свое дальнейшее развитие теория сетевых войн, которые ведутся не отдельными государствами или их коалициями, а новыми наднациональными глобальные структурами, появившимися в процессе информатизации общества на основе сетевых принципов мироустройства. Сетевое общество создается в процессе развития и совершенствования разнообразных информационных каналов [24], которые и составляют многочисленные социальные сети. Военные расходы и человеческие потери во время войн. Во второй половине XX в. в полный рост заявили о себе два важных фактора, которые изменили представление о войне и средствах ее ведения, а именно: закономерно выросли до гипертрофированных размеров военные расходы практически во всех странах мира, а также, что принципиально важно, появилось оружие массового уничтожения (ОМУ). Даже без ОМУ человечество теряло миллионы граждан, в новых условиях потери могут резко возрасти. Поэтому возникла потребность в новых средствах и способах решения задач обеспечения национальных интересов с меньшими потерями военнослужащих и гражданского населения, а также с меньшими финансовыми потерями.

Несмотря на то, что военные расходы и потери населения приобрели устрашающие размеры, тем не менее, причина противоборства государств сохраняется. Этому обстоятельству не мешает даже наличие ядерного оружия у ряда государств, так как обусловлено важным фактором – истощением минерально-сырьевых ресурсов и перманентным желанием ряда государств, и в первую очередь – США, к глобальному господству. Мировой опыт показывает, что в течение многих веков ресурсы всех видов были и остаются доминирующим побудительным мотивом походов и войн. Тому примеров множество и на эту тему издано большое количество научной литературы.

Применение традиционных войн и вооруженных конфликтов в настоящее время не прекращается. Более того, они становятся перманентными. Это и расчленение Югославии, и захват силой Ирака, подавление народов Сирии и Афганиста-

на, конфликт на Украине, другие большие и малые войны. Таким образом, используется смесь экономических и «вооруженческих» войн и конфликтов. Они порой меняются местами или существуют одновременно. Например, экономический кризис 1929–1933 гг. был разрешен во многом за счет роста милитаризации мировой экономики, а затем Второй мировой войны. Иногда малые войны помогают решать экономические задачи на континентальных территориях. Есть основания считать, что американцы пытаются дестабилизировать именно те страны, из которых Китай получает минеральные ресурсы, в том числе Ближний Восток. Есть и еще одна особенность военных кампаний, проводимых США и их союзниками: они происходили в непосредственной близости у границ СССР и современной России: Корейская война (1950–1953), война во Вьетнаме (1957-1975), Афганская война (1979–1989), война в Персидском заливе (1991), война НАТО против Югославии (1999), против Афганистана (2000), против Ирака (2003), против Ливии (2011). При этом силовые методы сосуществуют с экономическими методами воздействия. Так, в настоящее время США не только поставляют оружие так называемым сирийским повстанцам, но и прибегают к экономическим санкциям против Сирии, оказывают политическое давление на Сирию непосредственно или через страны-сателлиты НАТО.

1.3. Гибридные войны

Исторический анализ, проведенный в работах авторов [25] показывает, что государственная политика России и СССР в области национальной безопасности в послевоенный период строилась в основном на базе развития и поддержания боеготовности стратегических сил сдерживания, обеспечивающих гарантированный и неприемлемый ущерб потенциальному агрессору. Этот фактор на протяжении пяти послевоенных десятилетий обеспечивал определенное равновесие в мире и предотвращал перерастание политических и экономических конфликтов в военные.

Появление и практическое применение странами НАТО новых методов достижения политических и экономических целей в отношении ряда суверенных государств, основанных на дистанционном управлении конфликтами, привело к дестабилизации сложившихся международных отношений. Получившая распространение концепция гибридных войн позволяет добиваться стратегического преимущества по всем направлениям без масштабного применения не только ядерных, но и обычных вооружений. Причем затраты человеческих, материальных и иных ресурсов на проведение такого рода операций несоизмеримо ниже, чем при ведении контактных военных действий.

Преимущества, способствующие достижению поставленных целей, могут быть получены путем реализации комплексной программы, включающей в себя политику так называемой мягкой силы, переходящей в случае необходимости в более жесткую стратегию, связанную с экономическим, финансовым и информационным давлением. Следует отметить, что результаты реализации политики мягкой силы впоследствии достаточно легко трансформируются в базу для формирования агрессивных оппозиционных группировок, дальнейшая активизация которых в определенный момент времени, может привести к демонтажу экономической, финансовой и политической системы страны. Основными проводниками мягкой силы являются различные некоммерческие организации (НКО), контролируемые зарубежными спонсорами средства массовой информации, образовательные учреждения, религиозные организации, транснациональные корпорации и банки, которые ведут активную подрывную деятельность против органов легитимно избранной власти практически во всех развивающихся странах мира. Стратегия мягкой силы нацелена в первую очередь на морально-психологическую обработку населения, внушение элементов недоверия к действующим органам местной власти, формированию благоприятного образа вероятного противника. Результатом реализации данной стратегии может быть утечка за рубеж ценной информации, капиталов и специалистов, уклонение граждан этих стран от выполнения своих обязанностей, саботаж управленческих решений органов власти, организация социальных волнений, беспорядков и др.

Особую роль в современном противостоянии играют экономические угрозы, включающие в себя ограничения в международном сотрудничестве, инвестициях и во внешней торговле. В настоящее время внимание органов власти уделяется в основном ресурсному обеспечению оборонно-промышленного комплекса, хотя проблема представляется гораздо шире. Существует жизненно важная необходимость исследования проблемы национальной экономической безопасности во всех видах деятельности. Потеря конкурентоспособности отечественной экономики должна расцениваться так же, как и военное поражение на поле боя. Для выработки стратегии национальной экономической безопасности следует выделить экономические противоборства, включающие торговые войны, санкции, ограничения конкуренции в отдельную научную категорию, имеющую разные по значимости уровни развития. В настоящее время в этой важной научной области не существует единого понятийного аппарата, нет классификации разновидностей экономического противоборства и нет, соответственно научно обоснованных и эффективных методов достижения приемлемого уровня национальной безопасности. Следует отметить, что российские вузы готовят специалистов в области экономической безопас-

ности, однако их уровень ограничивается проблемами предприятия, региона и народного хозяйства, хотя экономические войны носят международный характер и затрагивают интересы разных государств. В итоге принятие решений о защите наших экономических интересов запаздывает, и отечественные предприятия несут ощутимые убытки.

В России нет координационного органа по вопросам национальной безопасности, который мог бы оперативно реагировать на возникающие угрозы не только в военной сфере, но и в области экономического, информационного и иного гуманитарного противоборства на международном уровне.

Исследования в области ведения гибридных войн проводятся в недостаточных объемах, и российская наука в области национальной безопасности ощущает дефицит в научных публикациях на эту тему. Несмотря на наличие крупных и авторитетных научных учреждений в области экономики, в нашей стране нет специализированных исследовательских институтов в области национальной экономической безопасности, хотя и имеются отдельные научные подразделения и специалисты в данной области.

В связи с этим, необходимо провести анализ и исследование процессов, вызванных враждебными действиями, изучить зарубежный и исторический опыт невооруженного противостояния государств, разработать методологию формирования государственной политики, способной адекватно реагировать на новые вызовы и угрозы в сфере национальной безопасности.

Необходимо разработать и научно обосновать стратегию, в которой Россия не только должна обороняться в развязанной против нее войне, но и вести наступательные действия при помощи реализации стратегии мягкой силы, результатом которых будут привлечение новых участников в военные, экономические, политические союзы, создание устойчивого положительного образа нашей страны как надежного партнера за рубежом.

Стратегия мягкой силы России за рубежом должна базироваться на инвестициях в реальный сектор экономики и человеческий капитал страны. В связи с этим, предлагается провести исторический анализ опыта СССР и США в сфере применения мягкой силы в отношении государств «третьего мира» в послевоенный период, на основании которого разработать принципы формирования внешнеэкономической политики России, адекватной современным угрозам и вызовам.

В течение XX–XXI вв. США реализовали несколько проектов по установлению контроля над рядом государств невоенными методами. Наиболее успешным можно считать смену режимов в Чили, Гватемале, Югославии, в странах Северной Африки и Ближнего Востока. При этом были использованы различные методы и

формы экономического и финансового давления, информационной блокады и других провокаций, которые привели к потере суверенитета этими странами.

Россия обладает колоссальными природными ресурсами, а также в состоянии привлечь значительные трудовые ресурсы для реализации крупных проектов. Несмотря на высокую степень износа основных производственных фондов, отечественная промышленность в состоянии в сжатые сроки решать важнейшие стратегические задачи. В качестве метода защиты следует рассматривать механизм реагирования на недружественные действия в отношении России невоенного характера со стороны военно-политических блоков система несимметричных мер ответного реагирования в отношении стран и зарубежных компаний, поддерживающих антироссийские санкции и мероприятия, с учетом потенциала России по разрешению конфликтов невооруженным путем.

1.4. Экономические войны

Экономические войны, как и большинство других, были всегда. Так, Афины в V веке до н.э. запретили торговые отношения своим гражданам с территориями, подконтрольными Спарте, что, в конечном счете, привело к падению влияния Афин. Экономические войны вели Карфаген в регионе Средиземноморья, Западная Римская империя с Венецией, Франция Наполеона Бонапарта против Англии, используя блокаду. Одной из разновидностей экономических войн являются военно-экономические блокады и санкции против неугодных стран. Например, в течение 20 лет применяются санкции против Ирана. Свободолюбивая Куба много лет испытывала блокаду со стороны США. Сейчас газовый проект «Северный поток» оказался в эпицентре энергетических войн. Учитывая складывающиеся тенденции можно считать, что в настоящее время против ряда стран, куда входят Россия, Китай, Иран ведется война, которую можно и нужно назвать финансово-экономической. В качестве синонима можно использовать термин экономическое противоборство. Такой точки зрения придерживается ряд политологов, которые считают, что мир имеет дело с новыми формами войны. В любой войне конечная цель – это обретение контроля. Поэтому нанесение удара по финансовому сектору может быть настолько эффективным, насколько это не сумел бы сделать ни один генерал, используя военные средства. Многие государства действительно находятся в состоянии войны, которая ведется с помощью не огнестрельного, а финансового и информационного оружия. ЕС выступает как механизм распространения на территории Европы влияния американских элит: американские банки контролируют европейскую финансовую систему, а американские военные занимают ответ-

ственные руководящие посты в НАТО. Так, в последние годы начала XXI в Европе все больше начинают возникать внутриевропейские финансовые «долговые войны», когда правительство ФРГ и его союзники создают условия для разрушения Европы и установления над ней контроля. Пример – Греция. Сегодня глобализация финансового рынка опаснее для международной стабильности, чем атомное оружие. Конечная цель любой войны состоит в обретении контроля, захвате территории и экономических ресурсов. Если этого удается добиться без вступления в открытое столкновение с противником, то победа становится еще более весомой. При этом поверженный противник может даже не заметить своего поражения. В современном мире финансовая система является сердцем экономики, основой постиндустриального общества, поэтому контроль над финансами дает власть, в том числе политическую. Главным средством борьбы в мире стал финансовый террор. Именно деньги поражают цели, в роли которых выступают страны – потенциальные противники. В современном мире главной стратегической ударной силой стали финансы. Итальянские ученые придумали особое направление – «геоэкономику». Они считают, что геофинансы являются главной составной частью современной геоэкономики. Именно в этой области ощутимее всего подрывается государственный суверенитет. Головным орудием финансовой войны выступает Международный валютный фонд (МВФ). Предоставление МВФ средств связано с выполнением странами–заемщиками определенных условий. Выделяемые кредиты имеют, как правило, жесткую направленность. При определенных обстоятельствах они могут способствовать свертыванию инвестиций, экономическому застою, снижению жизненного уровня населения. Есть и другие способы ведения финансовой войны. Например, Китай может дестабилизировать доллар США, переведя свои резервы в оборот долларов и сбросив доллары – тогда обменный курс доллара рухнет. Такое действие могло бы стать китайским ответом на военное окружение Вашингтоном Китая. За внешней однополярностью современного мира скрываются острейшие противоречия различных групп мировой олигархии. Иногда возникают громкие банковские скандалы, банкротства и др. Есть тенденция к нарастанию лавины таких скандалов, и «управляемый хаос» может перерасти в неуправляемую стихию. Есть основания считать, что кроме Ротшильдов и Рокфеллеров в мире имеются также другие влиятельные центры интересов. Например, Ватикан, который можно рассматривать не только как духовно-религиозный центр, но и как центр финансового влияния. На современном этапе экономические войны осуществляются также по направлениям «перекачивания мозгов», финансово-экономической экспансии и промышленного шпионажа [26]. Следует при этом иметь в виду, что утечка мозгов дорого обходится нашему государству. Во-первых, это связано с потерей средств,

потраченных на обучение и подготовку специалистов, во-вторых, государство недопроизводит продукт, создаваемый нашими специалистами после отъезда из страны.

Вопрос количественной и качественной оценки влияния санкционного режима на экономики различных стран и, в частности, на российскую экономику неоднократно поднимался в работах российских и иностранных ученых [27–31]. Более восьми лет насчитывает период действия санкций, введенных против России и связанных с событиями на Украине [32] (далее – российские санкции).

Российские санкции различаются по типам и характеру ограничений и являются примером, так называемых smart-санкций (от англ. smart – разумный, интеллектуальный; то есть точечные санкции против определенных лиц, компаний или секторов, ограничения на специфические виды транзакций). Российские санкции вводились поэтапно, начиная с марта 2014 г., при этом списки санкционных лиц и компаний расширялись непрерывно. В качестве ответной меры в августе 2014 г. Россия ввела эмбарго на поставки широкого спектра сельхозпродукции из западных стран (далее – контрсанкции). Детальную хронологию, трактовку и юридический анализ именно российских санкций также можно найти в специализированных источниках, посвященных данной теме. При анализе санкционного эффекта (или эффективности санкций) основной проблемой, на наш взгляд, является сложность количественной оценки их влияния. В подавляющем большинстве случаев точно определить их эффект крайне сложно по причине огромного количества факторов, одновременно влияющих (прямо и косвенно) на макроэкономические показатели. Зачастую анализ строится на агрегированных данных по международной торговле с санкционируемой страной, динамике ВВП до и после введения санкций, при этом в модель зачастую вводится бинарная dummy-переменная, характеризующая период до (значение 0) и после (значение 1) введения санкций, а эффект от санкций оценивается исследователем и присваивается соответствующий индекс. В частности, для российских санкций оценка их влияния осложняется тем, что текущий кризис сочетает множество факторов помимо санкционного (экономический кризис, шок на ресурсных и товарных рынках, локальный валютный шок и банковский кризис). В редких случаях, когда санкции введены относительно одномоментно, масштабны (поддержаны множеством стран, затрагивают целые секторы экономики) и относительно «просты» в трактовке (что не всегда характерно для smart-санкций) – оценка их эффективности может оказаться довольно точной. Так, например, санкции против Ирана, ограничивающие экспорт всей сырой нефти, довольно хорошо поддаются моделированию и анализу [33]. В рамках данного подхода предпринимается попытка построения простой модели индекса интенсив-

ности санкций, которая в определенной степени дорабатывает методику, предложенную К. Дрегером [34]. В частности, для оценки степени влияния различных типов санкций в зависимости от объема двусторонних торговых отношений с Россией по методике Дрегера включен эффект доли соответствующей валюты (доллар США, евро и др.) во внешнем долге санкционируемых секторов экономики, фактор крупности и системности санкционированных юридических лиц и финансовых организаций, а также роль санкционируемой страны в добыче трудноизвлекаемой нефти и газа (unconventional oil and gas) для технологических санкций.

Для проведения анализа воспользуемся Базой данных по санкциям и угрозам их введения за период 1945–2005 гг. (Threat and Imposition of Sanctions database, TIES), которая включает в себя информацию о целях отправителя санкций и приводит оценку экономических издержек от введения этих санкций. Обычно санкции классифицируют по основным видам или силе их эффекта. Здесь мы кратко приведем наиболее общую классификацию с разделением санкций на четыре основные группы:

1) дипломатические – отзыв посла, отказ от международных переговоров;

2) финансовые – ограничения на финансирование международными (МВФ, ВБ и другими организациями), запрет на инвестиции, замораживание активов;

3) торговые – торговые эмбарго, ограничения на импорт и экспорт групп товаров (например, военного или двойного назначения;

4) собственно smart-санкции – точечные санкции против определенных лиц, компаний или секторов, ограничения на специфические виды трансакций.

Российские санкции включают в себя ограничения из всех перечисленных групп. Для решения проблемы был выделен ряд наиболее «весомые» групп санкций, которые могут иметь непосредственное влияние на характеристики долгового рынка для реального сектора России:

- финансовые санкции (или секторальные, или так называемый SSI List – Sectoral Sanctions Identifications List), которые подразумевают ограничение доступа к рынкам заемного и акционерного капитала (в частности, ограничения ЕС и Директивы OFAC (Office of Foreign Assets Control of the US Department of the Treasury) и аналогичные ограничения других стран)
- технологические санкции, включающие ограничения в области технологий и услуг для разведки и нефтедобычи (в частности, Директива OFAC № 4 и аналогичные ограничения других стран);
- торговые санкции и ограничения на торговлю товарами и технологиями «двойного назначения»;

- санкции SDN (Specially Designated Nationals), которые подразумевают «замораживание» в США активов физических и юридических и де-факто запрещают проведение любых операций, имеющих прямое или косвенное отношение к США.

Среди последних работ, посвященных российским санкциям, можно отметить статью К. Дрегера «Влияние экономических санкций и цен на нефть на российский рубль», опубликованную в журнале «Journal of Comparative Economics», где результат санкций на обменный курс рубля оценивался на основе модели векторной авторегрессии. Анализ показал, что в основном динамику рубля определяют колебания цены на нефть, а не экономические санкции. Практический интерес в данной работе также представляет Индекс российских санкций, построенный авторами для дальнейшего использования в модели векторной авторегрессии. В настоящей работе мы предлагаем модифицировать данный Индекс для получения более точных оценок.

Следует отметить, что финансовые секторальные санкции запрещают, в частности, новое финансирование в долларах США на срок более 30 дней для банков (SSI Directive 1) и более 90 дней для SSI компаний (SSI Directive 2,3) в санкциях США, и в евро на срок более 30 дней в санкциях ЕС, размещение облигаций и ценных бумаг в соответствующих валютах и пр.

1.5. Технологические угрозы

Новые технологии и открытия, которые могут быть использованы в военных целях. Создание новых технологий и техники, в том числе новых средств вооружённой борьбы, определяет облик конфликтов на современном этапе.

Следует отметить, что временной период между началом фундаментальных исследований в конкретной области и внедрением их результатов в военную промышленность постоянно сокращается. Если с момента начала исследований в области ядерной физики до создания видов и родов войск, оснащённых ядерным оружием, прошло более 20 лет, то с момента начала исследований в области нанотехнологий до их внедрения в образцах новых видов вооружения, военной и специальной техники (ВВСТ) – менее 10. Таково следствие ускорения технологического цикла, причём, как отмечает А.А. Кокошин, это ускоряющийся процесс, требующий учёта и анализа научно-технических, политических, социально-экономических и военных факторов [35]. Поэтому в течение конечного времени его скорость формально должна достигнуть бесконечности, и всякие линейные прогнозы после этого будут невозможны. Наиболее высокие темпы ускорения внедрения результатов

фундаментальных исследований в военную промышленность демонстрируют развитые страны, использующие эффективные механизмы выявления из всего множества фундаментальных исследований тех, которые имеют наивысший потенциал с военной точки зрения. Такому подходу не мешает и глобализация, проявляющаяся в интернационализации науки – совместном выполнении крупных исследований, поскольку сами по себе знания лишь обеспечивают возможность создания соответствующей высокотехнологичной и высокоэффективной продукции как военного, так и гражданского назначения. Основное преимущество развитых стран заключается в том, что они, располагая значительными ресурсами и высоким производственно-технологическим потенциалом, способны осуществлять концентрацию знаний из различных областей. Последнее является необходимым условием трансформации научно-технического потенциала в фактор создания новых образцов ВВСТ.

Знания, получаемые российской наукой в результате участия в международных проектах, оказываются малопродуктивными, прежде всего из-за фрагментарности отечественного научно-технического потенциала, значительного отставания его отдельных составляющих от мирового уровня. Тенденция ускорения внедрения результатов фундаментальных исследований в военную сферу снижает возможности нашей страны реагировать на появление угроз от новых видов ВВСТ, поскольку если временной период в несколько десятилетий позволяет, оперативно перераспределив ресурсы, провести соответствующие исследования и получить готовые к внедрению результаты, то за десятилетний период аналогичный рывок осуществить практически невозможно. Помимо этого, усложнение науки создаёт ситуацию, когда достижение нового качества требует значительно большего количества исследований, причём сразу во многих областях – современные достижения рождаются в основном на стыке наук. Оценка текущего состояния фундаментальной науки указывает на следующие области, достижения которых могут стать основанием для создания новых вооружений [36]:

- единая теория поля (обещает появление методики выявления иных видов взаимодействия материи/энергии и экспериментальной проверки их существования, что откроет перспективу разработки принципиально новых систем ВВСТ);
- геофизика и климатообразование (предполагается появление средств, позволяющих оказывать достаточно мощное воздействие на геофизические факторы и климат практически в глобальном масштабе);
- генетика (значимые для военного дела разработки ведутся в направлении создания болезнетворных бактерий и вирусов с высокодифференцированной способностью поражения);

- квантовая оптика (создание малогабаритных генераторов сверхмощного излучения СВЧ-радиодиапазона, оптического и рентгеновского излучения является основным условием разработки целого семейства высокоэффективного лучевого оружия);
- вычислительная техника (за счёт применения телепортации квантовых частиц могут быть созданы относительно малогабаритные ЭВМ, обладающие гигантской производительностью, существенно превосходящей даже современные суперкомпьютеры);
- нанотехнологии (создание технических устройств наномасштаба с требуемыми функциональными возможностями и способностью к самовоспроизведению гарантирует появление качественно новых систем оружия, основанного на суспензиях нанороботов, позволяющих в короткие сроки уничтожать военные объекты, ВВСТ и живую силу противника).

Технологическая зависимость экономической системы. В современных условиях обострения международных экономических отношений проблема выживаемости России во многом будет зависеть от ее экономического развития. Особое внимание этой проблеме было уделено в Послании Президента Федеральному Собранию: «Технологическое отставание, зависимость означают снижение безопасности и экономических возможностей страны, а в результате – потерю суверенитета» [37]. Ранее принятая руководством страны Стратегия инновационного развития России ставила цель, заключающуюся в увеличении доли страны на мировых рынках высокотехнологичных товаров и услуг в таких видах деятельности, как атомная энергетика, авиастроение, космическая деятельность и др. [38], на реализацию которой было оказано санкционное давление со стороны группы индустриально развитых государств. Интегрированная в мировую финансовую и политическую систему, находящаяся под контролем США, Евросоюза и их сателлитов, экономика России оказалась в достаточно сложном положении. С момента реформирования российской экономики в 1990-е гг., в стране начали появляться и в настоящее время окончательно сформировались так называемые технологические угрозы, реализация которых представляет существенную опасность для развития отечественной наукоемкой промышленности. Данный вид угроз связан со сформировавшейся за последнюю четверть века повышенной чувствительностью российской промышленности к воздействию различных внешних факторов. В зависимости от характера воздействия, будем различать следующие типы угроз:

- зависимость в сфере управления производством (угрозы первого типа);
- зависимость в производстве средств производства (угрозы второго типа);

- зависимость от поставок материалов и комплектующих (угрозы третьего типа).

Угрозы в сфере управления производством (угрозы первого типа). Под контролем зарубежного капитала находятся российские предприятия с участием иностранных инвестиций, которые могут управлять производственными процессами посредством ограничений в сроках действия технологических лицензий, поставках комплектующих, программного обеспечения и т.п. Особую опасность представляет установка на отечественные стратегические предприятия зарубежных автоматизированных систем управления производством, которые не только открывают доступ к конфиденциальной коммерческой информации, но и позволяют контролировать хозяйственную деятельность.

Наиболее распространенной системой управления является программа ERP (англ. Enterprise Resource Planning, планирование ресурсов предприятия), которая представляет собой организационную стратегию интеграции производства и технологических операций, управления активами, трудовыми и материальными ресурсами. Характерной особенностью системы являются базы данных, содержащие подробную информацию о предприятии, его контрагентах, сотрудниках, оборудовании, финансах и других активах, которые размещены в специальных приложениях (модулях): финансы, логистика, кадры и т.д. Поставщиками системы ERP являются такие зарубежные корпорации, как немецкая SAP AG, американские Oracle, Microsoft, голландская Baan. Немецкая SAP захватила лидерство в этом сегменте мирового рынка информационных услуг еще в конце 1990-х гг., поставив свои программы автоматизации управления более 60% транснациональных корпораций.

На отечественном рынке IT технологий лидерами считаются 1С и Галактика. Среди зарубежных компаний, присутствующих на российском рынке можно выделить SAP AG, поставивший систему R/3 ERP крупным российским компаниям, имеющим стратегическое значение для экономики страны, а также государственным учреждениям и организациям. Разработки специалистов SAP и других компаний существенно расширили область применения системы ERP. Если в 1990-е гг. система ставилась в основном на промышленных и торговых предприятиях, то уже к началу 2000-х гг. были разработаны приложения для предприятий энергетики, коммунального хозяйства, связи, органами государственной власти, банков, страховых компаний и некоммерческими организациями.

Система R/3 ERP предусматривает установку в организации заказчика специального компьютерного оборудования, приспособленного для работы с программой, включающие в себя презентационные серверы, серверы приложений и серверы баз данных. Система может эффективно функционировать только после

того, как в нее будет закачена вся информация о предприятии, включая характеристики основного технологического и вспомогательного оборудования, технические характеристики и объем выпускаемой продукции, потребности в материалах, энергии, сведения о поставщиках и потребителях, личные данные о работниках и др. Как правило, такая работа ведется под контролем специалистов компании-поставщика, которые, естественно, получают доступ к конфиденциальной информации. В течение всего срока действия лицензии к организации-заказчику прикрепляется консультант поставщика, который отслеживает правильность функционирования программы, помогает решать различные проблемы, связанные с изменениями во внешней среде и внутри предприятия, устраняет возможные сбои в работе программы и т.д. Сопровождение программы обходится заказчику в десятки миллионов рублей ежегодно, а стоимость лицензии составляет, в зависимости от комплекса решаемых задач и масштабов деятельности предприятия, сотни миллионов рублей. Клиентами российского подразделения SAP являются крупнейшие промышленные предприятия, от результатов деятельности которых существенно зависят регионы и доходная часть федерального бюджета. SAP установил свое программное обеспечение на стратегических предприятиях отечественной промышленности и энергетики, таких как Череповецкий металлургический комбинат (Северсталь), Новолипецкий металлургический комбинат (НЛМК), Объединенная металлургическая компания (ОМК), КамАЗ, Роснефть НК, Калужский Турбинный завод (КТЗ), Газпром, Лукойл, Росатом и др. В сфере транспорта и связи клиентами SAP являются РЖД, Аэрофлот, МТС, Мегафон и другие сотовые операторы связи. Как можно заметить информация о функционировании гражданского сектора экономики, включая транспорт, связь, торговлю, промышленность полностью контролируется иностранными поставщиками программного обеспечения, что создает угрозу национальной экономической безопасности. Ситуация усугубляется еще и тем, что иностранное корпорации, специализирующиеся на автоматизации управления включили в сферу своих интересов органы власти и финансовую систему страны. Среди государственных организаций и учреждений клиентами SAP являются Почта России, Пенсионный фонд России, Центральный банк России, Аналитический центр при Правительстве Российской Федерации, Министерство промышленности и торговли РФ (Минпромторг), Федеральная налоговая служба (ФНС). Клиентами SAP являются и такие крупные финансовые организации, как Сбербанк РФ, Уральский Банк Реконструкции и Развития (УБРиР), Промсвязьбанк, АльфаСтрахование СГ и др. Зарубежная система уже внедрена в «Корпорации тактического ракетного вооружения», а в 2010 г. компания «Российские космические системы» также решила создавать автоматизированную систему управления про-

изводством на платформе SAP ERP. Такое решение вызывает беспокойство в связи с тем, что в базу данных системы будут занесены вся информация по контрактам компании с остальными предприятиями Роскосмоса, а это представляет определенную угрозу безопасности реализации космических проектов, имеющих важное стратегическое значение.

Наряду с SAP активно ведут себя на российском рынке и другие иностранные IT-компании, среди которых следует выделить американскую Oracle, в сферу влияния которой попали Государственный таможенный Комитет РФ, Федеральное казначейство Министерства финансов РФ, Банк Москвы, Росгосстрах, Ингострах, промышленные предприятия. Голландская Baan установила программное обеспечение на крупнейших авиационных предприятиях России: АО «КнААПО» (авиационное производственное объединение им. Ю. А. Гагарина в г. Комсомольское-на-Амуре) и в ОАО «НПК “ИРКУТ”», производящих военные самолеты и вертолеты. Перечень российских предприятий и организаций, принявших решение в пользу иностранного программного обеспечения постоянно растет с распространением облачных технологий, которые подразумевают поставку программного обеспечения по подписке, как услугу SaaS (Software as a Service — программное обеспечение как услуга). Преимуществом этой технологии является то обстоятельство, что пользователь не должен закупать серверы и иное оборудование, где обычно устанавливаются базы данных и программное обеспечение. Здесь вся информация о работе организации высылается на сервер провайдера, где происходит ее обработка. Поставщик ПО полностью управляет процессом, а заказчик получает обработанную информацию и доступ к функциям программы через установленное на своем компьютере приложение. У заказчика нет доступа к программе, он не может вносить туда изменения, копировать ее и т.п. Таким образом, разработчик ПО борется с нелегитимным распространением программы, а заказчик за сравнительно невысокие периодические платежи получает доступ к услугам. Поставщик облачной системы автоматизированного управления позволяет отключать некоторые временно ненужные функции или подключать на время дополнительные модули, что является несомненным преимуществом данной технологии для пользователя.

Однако, вместе с несомненными положительными моментами, которые предоставляют современные информационные технологии бизнесу и власти, имеется одно обстоятельство, которое ставит под сомнение их широкое использование. Появляется возможность для третьих лиц получать и использовать в своих интересах конфиденциальную информацию о деятельности предприятий, организаций, органов власти, которые воспользовались зарубежным ПО. Для клиентов технологи SaaS возможна ситуация, когда они могут частично потерять управление орга-

низацией. Если в классическом варианте у пользователя системой ERP есть возможность создавать копии файлов, редактировать информацию на собственных серверах, не уведомляя об этом провайдера, то при использовании облачных технологий, клиент получает от поставщика услуг только коды доступа к своим данным, которые в любой момент могут быть заблокированы. Провайдер может через определенное время изменить в свою пользу условия договора, передать конфиденциальные сведения о своих партнерах третьим лицам или совершить иные действия, несущие угрозу бизнесу заказчика.

Перечень угроз, связанных с использованием зарубежного программного обеспечения достаточно обширен и включает в себя утечку данных с предприятия до полной блокады работы предприятия в случае принятия санкционного решения в этом направлении. Учитывая то, что основными клиентами зарубежных разработчиков являются стратегические предприятия, деятельность которых оказывает существенное влияние на экономику России, следует с особым вниманием относится к выбору программного обеспечения.

Для повышения устойчивости экономики к внешним воздействиям необходимо срочно приступить к реализации программы импортозамещения в сфере информационных технологий. Программа должна включать в себя два раздела (подпрограммы) – создание ПО – отечественной системы ERP и выпуск специализированного оборудования. На российском рынке уже успешно функционируют отечественные программы автоматизации управления разработки 1С и Галактика, которые могут достаточно эффективно использоваться вместо ПО зарубежных поставщиков.

В соответствии с программой импортозамещения в России на базе федеральных ядерных центров уже создано производство суперкомпьютеров, способных решать различные задачи, в том числе и задачи по управлению стратегическими производствами и организациями. Как сообщил глава Государственной корпорации по атомной энергии «Росатом» С. Кириенко, уже осуществлена поставка 117 суперкомпьютеров стратегическим предприятиям по заказам Министерства обороны РФ, «Роскосмоса», «Объединенной авиастроительной корпорация» и атомной промышленности.

Следует отметить, что под действие российского законодательства о государственной тайне попадают организации, которые не только напрямую имеют отношение к военному делу, но и располагают сведениями о запасах полезных ископаемых, перспективных научных разработках, результаты которых могут использоваться в военных целях, инфраструктуре, о связях предприятий по кооперации, некоторых аспектах финансовой деятельности.

Угрозы для страны заключаются в получении доступа к информации и блокирование работы оборудования систем управления. Следует отметить, что любой программный или аппаратный сбой в работе системы вынуждает пользователя обращаться к разработчику, который, в зависимости от избранной им стратегии, может оказывать давление на заказчика. Важным является и то, что поставщик ПО или оборудования имеет возможность периодически «снимать» информацию о работе «открытых» предприятий и организаций, анализировать ее и, после обработки, получать представление о работе «закрытого» сектора экономики.

В связи с этим, для предприятий с государственным участием и госучреждений различных уровней управления следует ограничить использование иностранного программного обеспечения при наличии отечественных аналогичных продуктов. Особенное внимание следует уделить организациям, имеющих стратегическое значение для экономики страны и занимающихся разработкой и изготовлением вооружений, военной и космической техники. Ограничение должно касаться не только зарубежного программного обеспечения, но и иностранного компьютерного, сетевого и телекоммуникационного оборудования.

Технологические угрозы в производстве средств производства (угрозы второго типа). В условиях рыночных отношений большинство отечественных предприятий высокотехнологичного сектора экономики, обладавших в свое время уникальными технологиями и передовой материально-технической базой, оказались неконкурентоспособными на мировом рынке и в настоящее время стремительно теряют накопленный интеллектуальный потенциал. Падение конкурентоспособности продукции с высокой добавленной стоимостью связано с невозможностью качественно изготавливать сложные узлы и агрегаты с использованием морально и физически устаревшего оборудования, износ которого, по данным Росстата, превышает 50%, а средний возраст составляет порядка 12 лет [39]. Россию практически вытеснили с мирового рынка приборостроения, гражданского авиастроения, стремительно теряет свои позиции судостроение, ракетно-космическая промышленность и другие отрасли.

Производство средств производства, к которым относят машины и оборудование, включая высокоточные и многоцелевые станки, инструменты, является основой, на которой строится экономический суверенитет государства. Практически вся отечественная промышленность характеризуется высокой зависимостью от зарубежных поставок высокоточных станков и технологической оснастки. Производство машин и оборудования в России в настоящее время находится в глубокой депрессии (табл. 1), хотя именно это направление является одним из необходимых элементов стратегии технологической независимости национальной экономики.

Таблица 1

Производство металлообрабатывающих станков в Российской Федерации

Наименование	1990	2010	2011	2012	2013	2014	2015	2016
Станки металлорежущие, штук	74 171	2832	3280	3467	2945	3871	3367	4383
Станки токарные с числовым программным управлением, штук	18 056	129	195	166	137	227	204	337

Источник: данные Росстата.

В советский период практически все произведенное оборудование директивно распределялось по предприятиям, что решало ставшую актуальной в рыночной экономике проблему спроса. В СССР неоднократно предпринимались попытки копирования лучших зарубежных образцов техники, что приносило определенный результат, хотя и с некоторым отставанием в технических характеристиках. В настоящее время наверстать отставание в станкостроении пытаются с помощью предоставлений преференций зарубежным прямым инвесторам в строительстве и модернизации предприятий. В течение последних четырех лет были открыты и приступили к выпуску оборудования предприятия с участием иностранных инвестиций, среди которых филиал немецко-японского концерна «DMG Mori Seiki» в Ульяновске, инструментальный завод немецкой компании «Guhring» в Нижнем Новгороде, российско-чешское совместное предприятие «МТЕ Ковосвит Мас» по выпуску высокоточных станков в Ростовской области и др. Благодаря реализации государственной программы импортозамещения, удалось переломить негативную тенденцию и увеличить, начиная с 2014 г., выпуск станков и оборудования. Были закуплены лицензии на выпуск наиболее перспективных моделей станков. Новые технологии по сборке станков японской компании TAKISAWA были освоены на Ковровском электромеханическом заводе, в Екатеринбурге на базе компании «Пумори-инжиниринг инвест» открыто серийное производство японских металлорежущих обрабатывающих центров «Okuma».

Государственная поддержка заключалась в стимулировании спроса предприятий, участвующих в федеральных целевых программах. Как видно из табл. 1, в результате за три года удалось увеличить выпуск металлорежущих станков на 49%, а станков с ЧПУ почти в два с половиной раза по сравнению с 2013 г.

Вместе с тем, решить проблему спроса на внутреннем рынке пока не удается. Наши потребители по-прежнему предпочитают приобретать нужную им технику за рубежом, даже если имеются российские аналоги, объясняя свой выбор низким качеством отечественного оборудования, что не вполне соответствует реальному положению дел. Конкурентоспособность российской машиностроительной продукции подтверждается востребованностью отечественного оборудования на

мировых рынках. По данным Федеральной таможенной службы, экспорт оборудования в 2017 г. из России в страны дальнего зарубежья вырос почти на четверть (24,3% [40]) по сравнению с 2014 г., что свидетельствует о соответствии отечественной высокотехнологичной продукции мировому техническому уровню. Однако, отечественная промышленность пока не в состоянии закрыть дефицит в современном высокоточном и высокопроизводительном оборудовании, в котором остро нуждаются предприятия оборонной, авиационной и ракетно-космической промышленности. Недостаток предложения на российском рынке в многоцелевых станках, совмещающих максимально возможное число операций, а также программно-управляемых обрабатывающих центров, потребители возмещают на зарубежных рынках. Это обстоятельство вызывает определенное беспокойство, так как доминирование импорта на отечественном рынке машин и оборудования создает угрозу экономической безопасности страны. Анализ, проведенный авторами, показывает, что темпы роста импорта существенно превышают рост отечественного производства машин и оборудования, в результате чего российское машиностроение к началу 2018 г. оказалось практически вытеснено с национального рынка зарубежными конкурентами, не смотря на усилия правительства по реализации программы импортозамещения. С учетом того, что российские предприятия выпускают машины и оборудование, включающие в себя зарубежные узлы, приборы и агрегаты, следует признать практически полную зависимость отечественного машиностроения от зарубежных поставок. Одним из направлений частичного решения возникшей проблемы может стать разработка технологических процессов с уменьшенным объемом механической обработки. Тенденция к такому подходу наметилась достаточно давно, но развитие современных прогрессивных технологий позволяет считать их весьма эффективными. Разработка различных методов получения точных заготовок для изделий и сейчас уже позволяет значительно сократить объемы механической обработки. Здесь проблема состоит в том, что окончательная обработка проводится уже на высокоточном и особо высокоточном оборудовании, которое по себестоимости в разы превосходит оборудование нормальной точности.

Технологические угрозы, связанные с зарубежными поставками материалов и комплектующих (угрозы третьего типа). Следует отметить, что современные машины и оборудование комплектуются системами управления, состоящих из различных электронных приборов, датчиков, устройств памяти и т.п., имеющих, как правило, зарубежное происхождение. Зависимость отечественного машиностроения от импорта электронных приборов принимает критический характер. В предкризисный период (2007–2009 гг.) в стране сложилась ситуация, когда предприятия химической и нефтехимической промышленности, а также машиностроe-

ния и металлообработки не могли нормально функционировать без зарубежных поставок материалов, комплектующих и запасных частей к оборудованию, как показывает анализ, в группе «Машиностроение и металлообработка» в 2007 г. 53% исследованных предприятий имеют импортозависимость 100% по крайней мере по одному элементу продукции производственно-технического назначения. Следует отметить, что качественные характеристики, а, соответственно, и конкурентоспособность машин и оборудования, зависят от качества узлов, агрегатов и комплектующих входящих, в их состав. Замена оригинальных комплектующих на отечественные или зарубежные аналоги может существенно отразиться на качестве конечной продукции.

Современные модели электронных приборов, предназначенных для функционирования высокоточного оборудования, позволяют существенно улучшить характеристики продукции отечественного машиностроения, однако Россия значительно отстает в этом сегменте от конкурентов. В течение последних тридцати лет отечественные разработчики машин и оборудования, в основном, ориентируются в своих проектах на зарубежные электронные приборы и другие комплектующие, импорт которых зависит от различных внешних факторов. Так, в США действует специальный кодекс (ITAR International Traffic in Arms Regulations), регулирующий распространение технологий, которые могут быть использованы странами в военных целях. Введенные в 2014 г. экономические санкции в отношении России не позволяют передачу технологий, материалов и комплектующих двойного назначения, что представляет определенную угрозу инновационной модернизации национальной экономики. Пока санкционные ограничения касаются только оборудования и материалов двойного назначения, которые могут использоваться для изготовления военной и гражданской техники, однако санкции могут распространиться на другие виды деятельности и регионы, что представляет вполне реальную угрозу инновационному развитию российской экономики. Независимость от поставок зарубежных материалов и комплектующих российская промышленность может получить от реализации программы импортозамещения. Для развития отечественной радиоэлектронной промышленности есть очень хорошие перспективы, так как спрос на российском рынке существенно превышает предложение наших предприятий, производящих электронные приборы и ЭКБ. Однако, следует заметить, создание, практически с нуля, высокотехнологичных производств в условиях ограничения доступа к технологиям, требует колоссальных вложений капитала, что не под силу отечественным частным инвесторам. Поддержка государством предприятиям отрасли может быть реализована посредством финансирования программ инновационного развития. В 2007 г. была принята Федеральная целевая программа

«Развитие электронной компонентной базы и радиоэлектроники» на 2008–2015 гг., направленная на восстановление отечественных предприятий, имеющих стратегическое значение для инновационного развития России, ее обороноспособности и конкурентоспособности. Результаты реализации программы сделали реальной возможность разработать и изготовить достаточно широкий спектр приборов, включая микропроцессоры и контроллеры, а также силовую электронику, радиационно-устойчивые микросхемы и другую технику, незначительно уступающую зарубежным аналогам. Государственная программа «Развитие электронной и радиоэлектронной промышленности на 2013–2025 годы» предусматривает меры государственной поддержки предприятий, осуществляющих разработку базовых технологий производства приоритетных электронных компонентов и радиоэлектронной аппаратуры. Кроме того, предполагается компенсация части затрат на уплату процентов по кредитам, полученным в российских кредитных организациях на реализацию проектов по созданию инфраструктуры отрасли, в том числе кластеров в сфере радиоэлектроники [41].

Следует отметить, что по оценкам экспертов, прямое импортозамещение электронных приборов содержит элементы запрограммированного отставания. Практика показывает, что специалисты разрабатывают технологии или покупают лицензии на изготовление успешных образцов электронных приборов уже несколько лет использующихся в зарубежной технике. Учитывая, что каждые полтора–два года производительность микросхем удваивается, можно предположить, что изготовленная и укомплектованная устаревшими электронными приборами техника потеряет свою конкурентоспособность еще до начала своего выхода на рынок. За время разработки технологии и освоения новой машиностроительной продукции, зарубежные фирмы-производители электронной техники могут сменить несколько поколений приборов, на порядок отличающихся по своим характеристикам от скопированных образцов и вполне возможно, что заложенные в конструкции элементы могут быть уже сняты с производства. Таким образом, решить проблему импортозамещения путем копирования успешных зарубежных образцов вряд ли удастся. Для ликвидации отставания имеет смысл приобретать не лицензии на производство успешных образцов, а результаты перспективных научных исследований, на основе которых следует самостоятельно разрабатывать технологии для собственного производства.

Особое внимание государство должно уделять иностранным инвесторам, размещающим в России самое передовые производства по выпуску электронных приборов и ЭКБ по принципиально новым технологиям. Вкладывать ресурсы в освоение традиционных технологий изготовления микросхем в условиях быстрой

смены поколений электронных приборов не имеет смысла. Так, оптическая литография уже исчерпала свои возможности в технологиях электронного приборостроения. Известно, что длина световой волны находится в пределах 380–780 нм, а для ультрафиолетового излучения этот параметр составляет 10–380 нм. Таким образом, технологии 14 нм являются предельными в плане их дальнейшего совершенствования и приобретение (если продадут) лицензии, с учетом сроков освоения новых технологий на отечественных производствах, приведет к запрограммированному отставанию в развитии российской радиоэлектронной промышленности. Альтернативой оптической литографии можно считать технологию электронно-лучевой безмасочной литографии. В Москве введено в строй производство по лицензии голландской компании Mapper Lithography Holding B.V, в технологии которой экспонирование фоторезистивного слоя производится электронным пучком вместо света. Конкурентным преимуществом технологии Mapper по сравнению с оптической, является отсутствие дорогостоящих масок, которые в оптической литографии нужно изготавливать для каждого типа микросхем. Россия принимает участие в проекте Mapper Lithography в качестве исполнителя – поставщика приборов электронной оптики для оборудования по производству микросхем сверхмалого размера.

Технологические угрозы представляют серьезную опасность для российской экономики и, в связи с этим, государство должно принять адекватные меры по их нейтрализации.

1.6. Киберугрозы

Кибератака – это покушение на информационную безопасность компьютерной системы. Выделим следующие формы кибератак.

Кибертерроризм. Финансируется заинтересованными организациям и государствами и включает крупномасштабные мероприятия, направленные на получение секретных данных или нарушение функционирования ключевых систем крупных организаций или государств.

Киберрэкет. Финансируется заинтересованными организациями либо из собственных источников. Совершается в целях кражи данных, нарушения функционирования системы, шифрования и требования выкупа за возобновление работы системы.

Бытовые кибератаки. Чаще всего финансируются из собственных или заемных источников. Как правило, это мелкое мошенничество, осуществляемое в целях кражи денежных средств с банковской карты, кражи личных данных для получения

информации об объекте кибератаки, либо в целях получения выкупа. Последствия кибератак ежегодно исчисляются миллиардами долларов.

Выделяют следующие виды последствий кибератак.

Кража конфиденциальной информации. Утечка данных, содержащих информацию о патентах, технологиях, поставщиках, контрагентах, данных, являющихся коммерческой тайной, интеллектуальной собственностью субъекта.

Ущерб репутации. Факт успешно совершенной кибератаки формирует негативный образ уязвимой компании, с которой опасно сотрудничать.

Мошенничество. Непосредственная кража материальных ресурсов организации посредством доступа к банковским счетам или имуществу объекта кибератаки.

Судебные разбирательства. Разбирательства в суде неминуемо приведут к существенным расходам в связи с рассмотрением и разрешением судебного дела.

Упущенная выгода. Блокировка информационных систем компании неизбежно ведет к торможению всех бизнес-процессов и к снижению эффективности основной деятельности объекта кибератаки. Наиболее популярными видами кибератак являются следующие:

- атаки на web-приложения (SQL инъекции/XSS);
- 24% – внедрение вредоносного кода;
- 19% – атаки на приложения;
- 19% – DDS/DDoS-атаки (перегрузка сервера большим числом запросов);
- 9% – разведывательные атаки: активные (поиск конфиденциальной информации в системе жертвы) либо пассивные (поиск конфиденциальной информации вне системы жертвы);
- 9% – остальные виды атак – 20%.

Распространение вредоносных вирусов. Одним из самых заметных вирусов, распространяемых по электронной почте, стал вирус Mellisa – первый вредоносный код, который нарушил работу почтовых серверов многих крупных компаний мира. Вирус распространялся волнообразно, создавая огромный поток инфицированных писем. Ущерб от этой «эпидемии» оценивают в 80 млн долл.

Одна из первых масштабных DDoS-атак была совершена в 2000 г. посредством вируса Mafiaboy. Атака была инициирована канадским школьником, объектом стали несколько популярных сайтов, включая Amazon, Dell, Yahoo, Fifa.com, eBay и CNN. Ущерб оценили примерно в 1,2 млрд долл. Среди отечественных исследований проблем DDoS-атаки следует выделить работу Е.А. Гавриловой «Исследование методов обнаружения сетевых атак», в которой проанализированы раз-

личные методы компьютерных атак, а также способы их выявления и представлены возможные решения проблемы обнаружения вторжений [42].

Первым вирусом, оказывающим воздействие на мобильные устройства, был Cabir, появившийся в 2004 г. На экранах телефонов, зараженных данным вирусом, высвечивалась надпись Caribe. Вирус был замаскирован под ПО для защиты мобильных устройств от вирусов – Caribe Security Manager, которую пользователь должен был установить самостоятельно. Первым вирусом, распространяемым через социальные сети, стал ZeuS. Началось заражение в 2007 г. путем рассылки в социальной сети Facebook фото со ссылкой на веб-сайт, содержащий троянскую программу. Эта программа внедрялась в систему, добывая злоумышленникам регистрационные данные пользователя, позволявшие похищать средства со счетов клиентов ведущих европейских банков. Кибератака затронула пользователей Италии, Германии, Нидерландов и Испании. Самым известным вирусом, поражающим системы управления производственными процессами, стал Stuxnet. Данный вирус – это первое в мире, использованное в военных целях кибероружие, которое в 2009 г. вывело из строя 1368 ядерных центрифуг в Иране, разрушив всю их инфраструктуру, что отбросило ядерную программу Ирана на годы назад.

Серьезный ущерб был нанесен распространением вируса Lazarus, который в 2014 г. привел к массовой утечке личных данных из электронной почты работников компании Sony Pictures, а также к потере неизданных фильмов киностудии. Ущерб компании оценен в 100 млн долл. США. В 2016 г. на российские информационные ресурсы было совершено более 50 млн кибератак – это в три раза больше, чем в 2015 г. Более 60% атак производится из-за границы, с территории иностранных государств. Так, в первой половине 2017 г. были выявлены две крупные эпидемии вирусов шифровальщиков-вымогателей – WannaCry и NotPetya/ExPetr. Общий ущерб от последствий только этих двух крупных эпидемий оценивают более чем в 1 млрд долл. Вредоносная программа WannaCry была детально проанализирована Н.Е. Кувшиновым, А.А. Галяутдиновым [43]. Вирус атаковал 200 тыс. компьютеров, серьезные убытки понесли 150 стран. Он проникал в компьютеры с операционной системой Windows с устаревшими обновлениями, взламывал и зашифровывал жесткие диски и требовал 300 долл. за разблокировку системы. Воздействию вируса подверглись не только компьютеры и мобильные устройства частных лиц и организаций, но и объектов критической инфраструктуры – больниц, в которых были заблокированы различные устройства, включая медицинское оборудование. Кроме того, некоторым заводам пришлось остановить производство в связи с зашифрованным производственным оборудованием. При этом самой дорогостоящей кибератакой является отнюдь не эпидемия WannaCry, а эпидемия шифроваль-

щика NotPetya, также известного как ExPetr. Его принцип действия был схожим – проникновение, шифрование и требование выкупа. Однако в отличие от WannaCry, жертвами NotPetya стали организации, поскольку у создателей данного вируса был доступ к центру обновлений финансового программного обеспечения MeDoc, которое хозяйствующие субъекты использовали в своей деятельности.

1.7. Коррупция и нелегальное финансирование бизнеса

Серьезную угрозу для безопасности экономической системы представляет коррупция. Сопоставимые потери и издержки от безнаказанной коррупции «эффективных» менеджеров и финансистов в отношении объектов Сочи-2014, проекта ГЛОНАСС, реформ в Минобороны России, проектов Саммит АТЭС-2012, Сколково, Роснано и т.д. колеблются в пределах от десятков миллионов до десятков миллиардов рублей. Огосударствление управления РАН, резкое ограничение академических свобод и самоуправления, без сомнения, отрицательно скажется на эффективности академической науки. В российских реалиях, в частности, с учётом коммерческих интересов в отношении движимого и недвижимого имущества, активов и земли академии, это приведёт к бюрократизации и взрывному росту коррупции. Новая институция – Федеральное агентство научных организаций – не является новацией для России. В ходе реформ федеральной исполнительной власти в 2004−2005 гг. для управления наукой в структуре Минобрнауки России было создано Федеральное агентство по науке и инновациям (Роснаука), ведавшее деньгами и имуществом российской науки. Агентство просуществовало вплоть до 2009 г. и было упразднено за ненадобностью и неэффективностью. Повторный опыт организации подобных структур носит явные признаки традиционного «хождения по граблям» с умножением издержек. Урезание финансово-экономического и имущественного потенциала Российской академии наук предполагает последующее перераспределение, как функций, так и материального обеспечения между различными институтами фундаментальной и прикладной науки, институтами инноваций.

Общим для всех коррупционных схем является финальная стадия, на которой осуществляется вывод из оборота активов и их последующая легализация. Традиционно, для незаконного перевода капитала за рубеж использовались трансграничные торговые операции, когда для реализации фиктивного контракта было необходимо перевести зарубежному партнеру (как правило, оффшорной фирме) авансовые платежи, которые потом списывались как штрафы в убытки российской компании. Популярностью пользовались и схема оплаты фиктивных консалтинговых услуг, оказываемых иностранными фирмами. Для перевода капитала за рубеж

использовался механизм иностранного инвестирования. Одна из схем предполагала использование ценных бумаги, права на которые учитывались в зарубежном депозитарии. При продаже таких бумаг деньги переходили на иностранные счета. Другая использовала установленную Законом РФ «Об иностранных инвестициях» возможность беспрепятственного перевода доходов иностранного инвестора (репатриация прибыли) от хозяйственной деятельности в России [44].

В настоящее время широкое распространение получили такие финансовые инструменты вывода средств за рубеж, как криптовалюты.

Криптовалюты – это электронные деньги или цифровые активы, которые создаются частными компьютерными системами без контроля центральных банков. Самая известная криптовалюта на сегодняшний день – биткоин. Целью создания данной системы было введение в оборот нового средства платежа, при помощи которого его обладатели смогут обменивать добытые ими биткоины на товары и услуги. Продавцы этих товаров и услуг согласны принимать биткоины к оплате, потому что уверены в том, что в будущем также смогут тратить полученные ими биткоины на другие товары и услуги. То есть изначально биткоины создавался как альтернативная валюта. Как и другие современные валюты, биткоин не обеспечен реальными активами, а основан на доверии сторон, принимающих его в качестве оплаты, что затрудняет контроль за его оборотом со стороны государства. нелегальные трансакции могут сопровождать не только коррупционные схемы, но и финансировать терроризм и другую противоправную подрывную деятельность, что создает серьезную угрозу для любой социально-экономической системы.

ГЛАВА 2.
ПОДХОДЫ К ПОСТРОЕНИЮ СИСТЕМЫ БЕЗОПАСНОСТИ ЭКОНОМИЧЕСКОЙ СИСТЕМЫ

2.1. Принципы формирования стратегии безопасности экономической системы

Экономическая система не может нормально развиваться в условиях военной, финансовой и социальной нестабильности, в связи с чем, государство должно обеспечить соответствующую защиту, адекватную формирующимся во внешней и внутренней среде угрозам. Оборонный и экономический потенциал, как элементы системы тесно связаны между собой и не могут функционировать самостоятельно, отдельно друг от друга. Государство может иметь собственные вооруженные силы или ориентироваться на своих союзников, которые за определенную плату могут обеспечивать военную безопасность. В целях обеспечения национальной военной безопасности государство может реализовать следующие стратегии:

a) развитие национальной армии, оснащенной преимущественно собственным вооружением;

b) развитие национальной армии на базе зарубежного вооружения;

c) полная передача оборонительных функций другому государству или группе стран (союзникам);

d) частичная передача оборонительных функций союзникам.

Первая стратегия (a), основанная на развитие собственных вооруженных сил (ВС) и поддержание их боеготовности на достаточном для защиты уровне предполагает оснащение войск всеми видами современных вооружений, изготовленных и разработанных на отечественных предприятиях оборонного комплекса. Возможна закупка некоторых комплектующих и материалов за рубежом в ограниченных объемах для обеспечения эффективности производственного процесса. Реализация данной стратегии требует значительных затрат всех видов ресурсов, наличие хорошо оснащенного научно-производственного комплекса, образовательных учреждений специального профиля, полигонов и другой инфраструктуры.

Стратегия защиты государства может базироваться на национальных вооруженных силах, которые используют зарубежные вооружения (b). Как правило, такие страны не обладают мощным научно-производственным комплексом и инфраструктурой, необходимой для проведения научных исследований и разработок

в оборонных целях. Наличие полезных ископаемых или других ресурсов дает возможность государству, располагающему соответствующими финансовыми возможностями, приобретать вооружение, технику и амуницию за рубежом. В этом случае страна покупает наиболее перспективные образцы вооружений, которые отвечают требованиям национальной безопасности. Такая стратегия позволяет с одной стороны, избежать рисков, которые неизбежны при создании, испытании и эксплуатации новой техники, с другой существенно снизить расходы бюджетных средств и сократить цикл разработки-производство-эксплуатация.

Стратегия, основанная на полной (c) или частичной передачи (d) оборонительных функций союзникам. С целью защиты, правительство может вступить в альянс или иное союзное объединение с другими государствами, в котором функции защиты частично или полностью передаются партнерам. Как правило, этой платой являются экономические ресурсы союзника или его суверенитет, в качестве которых могут выступать местные товарные рынки, которые уходят подконтрольным союзнику корпорациям, месторождения полезных ископаемых, трудовые, энергетические и другие ресурсы. На территории государства и прилегающей акватории могут размещаться военные базы материально-технического снабжения, разведывательные центры, аэродромы, различные системы вооружения. При этом собственные вооруженные силы носят, как правило, бутафорский характер.

Страна, на территории которой расположены военные базы других государств, как правило, теряет самостоятельность в выборе направлений развития и вынуждена действовать в рамках политического и экономического курса своих зарубежных партнеров. Стратегии, основанные на полной или частичной передаче оборонительных функций союзникам, могут быть приемлемы для небольших стран и территорий, которые в силу своего низкого научного и производственного потенциала, не могут обеспечить полноценную защиту своей экономической системы.

В трудах ряда отечественных ученых отмечается, что основным и общепринятым признаком государства является суверенитет [45–47] и его утрата ставит под сомнение существование данной политической общности граждан. Стране, обладающей значительными природными ресурсами и претендующей на роль лидера в формирующемся многополярном мире, реализовывать данные стратегии (c; d) не имеет смысла.

На наш взгляд, актуальными являются стратегии, основанные на национальных вооруженных силах (a, b), которые могут использовать отечественное или зарубежное военное оборудование, технику и снаряжение.

Использование зарубежных вооружений позволяет государству сосредоточиться на завершающих стадиях жизненного цикла – освоение и эксплуатация во-

енной техники. Такая стратегия позволяет правительству с одной стороны сократить время и расходы на научные исследования, разработки и производство, а с другой – можно выбрать на мировом рынке вооружений самые эффективные средства достижения военных целей. Следует отметить, что сложные технические устройства, к которым относятся современные вооружения, нуждаются в специальных расходных материалах, запасных частях, инструментах и приборах, которые потребуются для проведения регулярных ремонтно-профилактических работах, что формирует определенную зависимость от зарубежных поставщиков. Кроме того, государство-заказчик вооружений, вынужден раскрыть сведения, касающиеся собственного оборонного потенциала. Необходимо учитывать и неизбежные контакты военнослужащих с представителями государства-поставщика вооружений, что может привести к утечке конфиденциальной информации. Не следует исключать и возможные «закладки» в аппаратуру и системы управления военной техникой, которые могут транслировать ее местонахождение, снижать характеристики или вовсе блокировать работу устройства по спутниковым или иным сигналам. Эти и другие факторы создают угрозы безопасности государства, хотя данная стратегия развития вооруженных сил может использоваться в переходный период, когда наблюдается смена поколений военной техники. Не представляет серьезной опасности закупка зарубежной амуниции, автомобильной техники, беспилотных летательных аппаратов (БПЛА), индивидуальных аппаратов связи, средств наблюдения (бинокли, прицелы, тепловизоры), спасения (парашюты, резиновые лодки, аквалангги) и защиты (противогазы, бронежилеты, шлемы), медицинских материалов, комплектов (аптечек), а также палатки, спальные мешки, бинокли и другие элементы военного (двойного) назначения, не имеющие решающего значения в боевой обстановке.

В условиях обострения международной обстановки в Европе и глобальной финансовой нестабильности, органам управления необходимо прикладывать максимальные усилия для создания надежной системы безопасности, однако дальнейшее наращивание государственных инвестиций в развитие ОПК и увеличение оборонного бюджета создает серьезную угрозу реализации ряда социальных программ и национальных проектов.

В связи с этим, стратегия формирования системы безопасности должна строиться на следующих принципах:

1. Система безопасности не должна быть дорогой, ее формирование и содержание не может ущемлять интересы и потребности граждан и бизнеса. Обострение международной обстановки в мире и особенно на границах государства неизбежно влечет финансовую нестабильность, в условиях которой вырастает

нагрузка на банки, промышленные предприятия, инфраструктуру. Увеличение налогов или сокращение социальных программ может разбалансировать экономическую систему, вызвать неприемлемую, в условиях нестабильности, социальную напряженность.

2. Система безопасности должна быть гибкой. Способность системы оперативно перестраиваться в зависимости от вектора давления дает возможность своевременно реагировать на формирующиеся во внешней среде угрозы. Гибкая система безопасности должна обладать свойством перебрасывать ресурсы с одного направления на другое. В холодной фазе конфликта ресурсы направляются на инновационное развитие, образовательные и другие социальные проекты, в результате реализации которых формируются стратегические резервы экономической системы. В горячей фазе эти резервы могут быть использованы для физической защиты жизненно элементов системы – территории, населения, промышленных объектов и т.п. Научный, промышленный и человеческий капитал, необходимый для развития экономической системы должен быстро перестраиваться для ее защиты в случае перехода конфликта в горячую фазу. Государство должно всячески поддерживать предприятия, выпускающие продукцию (услуги) двойного назначения, а также объекты промышленной и социальной инфраструктуры, которые могут использоваться в военных целях (склады, коммуникации, медицинские учреждения, базы отдыха и т.п.).

3. Система безопасности должна быть эффективной. Соотношение затрат на содержание системы безопасности и ожидаемого результата должно быть минимальным. Под результатом безопасности можно понимать предотвращенный ущерб от действий противника (введение торговых ограничений, перекрытие коммуникаций, изоляция банковской системы, замораживание и конфискация активов, а также прямой ущерб от военных действий).

Содержание собственных вооруженных сил, исследовательских организаций и производств оборонного комплекса требует значительных расходов, в связи с чем проблема эффективности используемых на эти цели средств приобретает особую актуальность. Мероприятия по повышению эффективности инвестиций в ОПК позволят добиться двух очень важных результатов:

- снизить объемы государственного финансирования оборонных проектов и программ;
- сократить начальные этапы жизненного цикла военной техники.

Достичь этих результатов можно, на наш взгляд, следующими путями:

- привлечением частных инвесторов в финансирование инвестиций ОПК;
- диверсификацией предприятий ОПК;

- привлечение гражданских предприятий к разработке и производству продукции двойного назначения.

Частые инвестиции в ОПК могут быть направлены в следующие проекты:

- освоение военных технологий в гражданском секторе экономики;
- покупка Минобороны услуг гражданских предприятий;
- передача в аренду части собственности Минобороны;
- выпуск Минобороны облигаций и других ценных бумаг для привлечения капитала частных (физических лиц).

Методы повышения эффективности инвестиций в ОПК будут подробно изложены в следующих разделах.

Основная цель стратегии защиты экономики – обеспечение ее жизнеспособности в различных состояниях внешней и внутренней среды. Мероприятия, разрабатываемые в рамках стратегии безопасности, должны быть адекватны угрозам, которые формируются во враждебных средах. Для нивелирования внешних военных угроз необходимо укреплять собственные вооруженные силы и оборонно-промышленный комплекс. Влияние финансово-экономических санкций и ограничений может быть снижено за счет развития науки, собственной промышленности, повышения уровня технологического суверенитета.

Структурная схема системы безопасности экономики представлена на рис. 1.

Основными элементами системы безопасности экономики являются:

- силовой блок, куда входят вооруженные силы, органы безопасности и другие ведомства, которые непосредственно противостоят угрозам прямого военного вторжения и гибридным атакам;
- предприятия оборонно-промышленного комплекса (ОПК);
- гражданский сектор, который обеспечивает ресурсами экономическую систему;
- научно-исследовательские организации, которые обеспечивают вооруженные силы, предприятия гражданского сектора экономики и ОПК современными разработками, позволяющими нивелировать угрозы:
- систему информационной безопасности.

Элементы системы связаны между собой, объединены одной целью и не могут существовать отдельно. Все элементы системы безопасности можно условно разделить на прямые и косвенные. Вооруженные силы и органы безопасности напрямую вступают в соприкосновение с противником и наносят ему моментальный физический ущерб. Экономические контрсанкции, торговые и инвестицион-

ные ограничения в отношении недружественных государств, господдержка импортозамещения и другие меры позволяют вытеснить конкурирующие компании с рынков и наносят противнику косвенный ущерб, который проявляется в течение длительного периода времени.

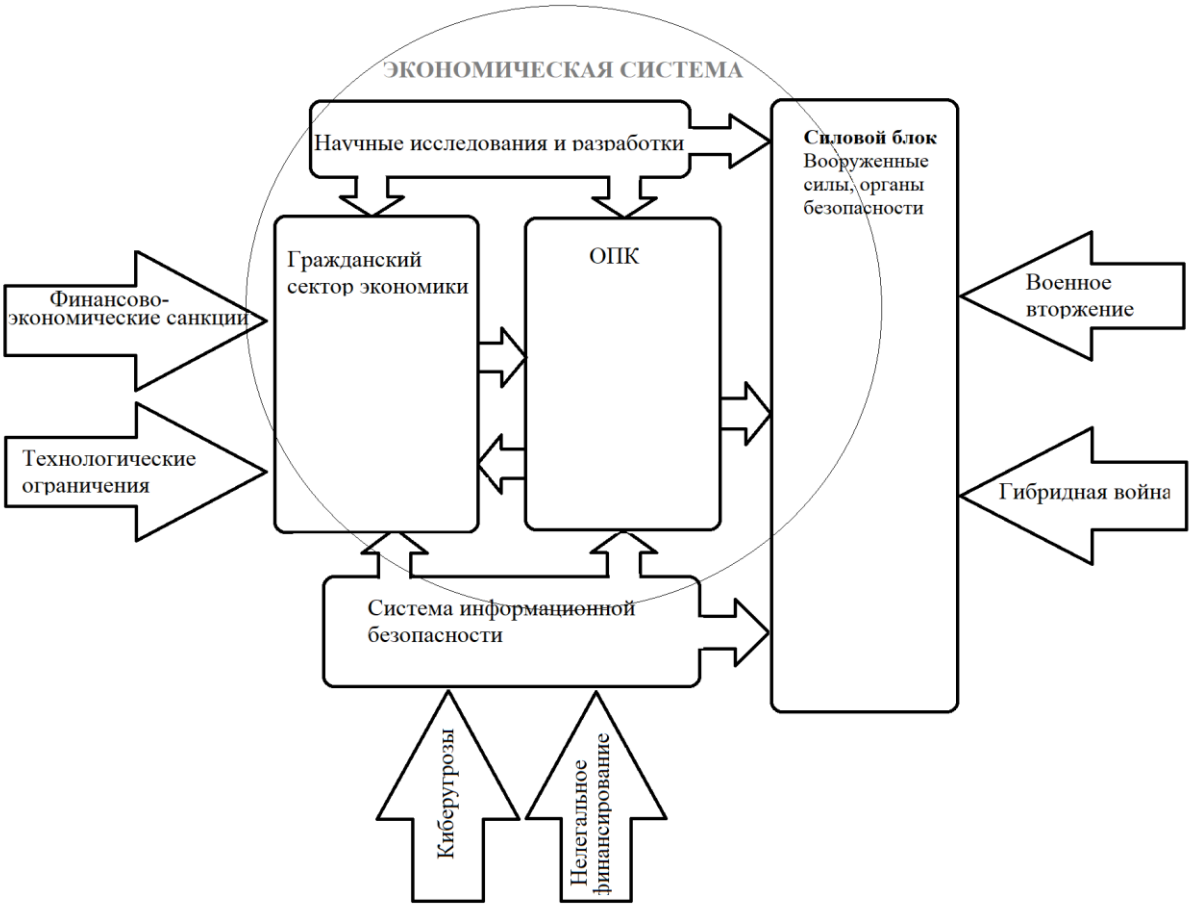

Рис. 1. Структурная схема системы безопасности экономики (составлено авторами)

2.2. Подходы к планированию развития силового блока системы безопасности

Вооруженные силы входят в силовой блок, обеспечивающий безопасность государства и играют решающую роль в защите социально-экономической системы от прямого воздействия внешних сил. Для развития этого важного элемента безопасности государства необходимо эффективно использовать все имеющиеся в экономике ресурсы. Эта проблема может быть решена с использованием методов программно-целевого планирования. Применительно к Вооруженным силам РФ, подходы к планированию двух основных составляющих их боевого потенциала, схема связи целей, задач и ресурсов представлены на рис. 2.

Рис. 2. Схема связей при программно-целевом планировании:

ГПВ – государственная программа вооружения; ГОЗ – государственный оборонный заказ; ОНР – основные направления развития; ПФП – перспективный финансовый план; ВВСТ – вооружение, военная и специальная техника; ВТС – военно-техническое сотрудничество; ФБ – федеральный бюджет; СП – социальные потребности: денежное довольствие, заработная плата, продовольствие, жилье и др. [47]

Общая процедура планирования развития вооруженных сил содержит следующие основные этапы:

1) оценка динамики военно-политической ситуации (функция политики);

2) формирование боевых задач военными специалистами;

3) оценка потребных ресурсов (ВВСТ, другая продукция военного назначения, капитальные сооружения), социальные потребности (денежное довольствие, заработная плата, продовольствие, жилье и др.), потребности в ВВСТ в интересах ВТС.

Одновременно производится оценка возможностей экономики, в том числе разрабатывается бюджетный прогноз Российской Федерации на долгосрочный период, что является принципиально новым. На различных этапах развития в органах государственного управления (Совет Безопасности, Государственная Дума, федеральные органы государственной власти) происходит согласование возможностей

и потребностей, завершающееся принятием федеральных законов о федеральном бюджете.

Оценка динамики военно-политической ситуации, осуществляемая политиками, включает в себя прогнозирование и анализ развития военно-политической обстановки на глобальном и региональном уровне, а также состояния межгосударственных отношений в военно-политической сфере с использованием современных технических средств и информационных технологий. При этом необходимо учитывать требования такого документа, как Стратегия национальной безопасности Российской Федерации, который является базовым документом в области планирования развития системы обеспечения национальной безопасности Российской Федерации [47].

Результаты анализа позволяют оценить и сформулировать основные внешние и внутренние военные опасности и угрозы государству. К их числу можно отнести наращивание силового потенциала Организации Североатлантического договора (НАТО) и наделение НАТО глобальными функциями, реализуемыми в нарушение норм международного права, приближение военной инфраструктуры стран – членов НАТО к границам Российской Федерации, в том числе путем дальнейшего расширения блока.

На основе данных, предоставляемых специалистами по военно-политическому анализу, осуществляется военное планирование, которое включает в себя определение порядка и способов реализации целей и задач развития военной организации, строительства и развития Вооруженных сил РФ, других войск и органов, их применения и всестороннего обеспечения. В результате формируются военные задачи, такие как, например, неядерного сдерживания, обороны территории Севера. Реализация задач осуществляется на основе оснащения Вооруженных сил РФ, других войск и органов вооружением, военной и специальной техникой, предусмотренных в государственной программе вооружения, в которой содержатся в частности:

- оценка рисков социально-экономического развития и угроз национальной безопасности Российской Федерации;
- поэтапные прогнозные оценки вероятного состояния социально-экономического потенциала и национальной безопасности Российской Федерации.

Важность создания документов по программному планированию подчеркивает положение закона о стратегическом планировании Российской Федерации о том, что порядок разработки, утверждения и реализации Государственной программы вооружения, а также сама программа утверждаются Президентом РФ. Таким образом, на современном этапе необходимо, прежде всего:

- повысить роль перспективного финансового плана в бюджетном процессе;
- совместными усилиями институтов Минобороны России и оборонной промышленности разработать методологию и совокупность методов долгосрочного прогнозирования показателей состояния экономики и затрат по этапам жизненного цикла образцов и систем вооружения, военной и специальной техники;
- активизировать работу по совершенствованию механизмов применения программно-целевых методов при планировании и осуществлении бюджетных расходов;
- перейти практически к распределению бюджетных ресурсов между администраторами бюджетных расходов исходя из поставленных перед ними целей и задач;
- особое внимание уделять формированию системы реальных и объективных индикаторов достижения администраторами бюджетных расходов поставленных целей и решения определенных, четко сформулированных задач.

Основными принципами формирования ресурсного обеспечения оборонных программ являются:

1) системность, в соответствии с которой военная организация должна рассматриваться как единая система, имеющая общее целевое предназначение. Планирование строительства и развития Вооруженных сил РФ осуществляется в соответствии с их ролью и местом в структуре военной организации государства;

2) иерархичность, в соответствии с которой цели развития Вооруженных сил РФ и их подсистем должны соответствовать целям развития системы более высокого уровня;

3) итерационность, в соответствии с которой процесс формирования военного бюджета должен учитывать сложную многоуровневую иерархическую структуру военной организации;

4) эффективность, в соответствии с которой объемы ассигнований, выделяемых на развитие различных компонентов военной организации, должны определяться исходя из вклада каждого из них в достижение целей вышестоящего уровня. Изложенный подход обеспечивает распределение военных расходов по задачам и программам строительства Вооруженных сил РФ, а также выделение ресурсов по видам Вооруженных сил РФ, родам войск (сил), военным округам и другим распорядителям бюджетных средств Министерства обороны РФ.

Такой метод разработки военного бюджета жестко увязывает его с системой планирования в Министерстве обороны РФ и создает необходимый финансовый инструмент для управления и контроля за реализацией планов и программ строительства и развития Вооруженных сил РФ [47].

В войсковом звене (уровень соединений и объединений) также должен реализовываться алгоритм: цель (задачи) – мероприятия – ресурсы. Например, такая задача, как подготовка личного состава до заданного уровня овладения практическими навыками. В соединении составляются планы, где формулируются цели и задачи деятельности, в том числе по боевой подготовке. Мероприятия включают боевую учебу, создание материальной базы, учения и др.

Содержание программы развития вооружения, военной и специальной техники определяют следующие группы факторов:

1) военно-политические факторы, отражаемые в Концепции национальной безопасности РФ. Они определяют приоритеты обеспечения национальной безопасности, внутренние и внешние угрозы. Так, важно определить, что опаснее – мировой терроризм, ядерная угроза, национальный экстремизм либо иные угрозы. Военная доктрина РФ, Основы государственной политики РФ по военному строительству также позволяют сформулировать боевые задачи видов Вооруженных сил РФ, родов войск, тактико-технические параметры отдельных образцов и систем оружия;

2) экономические факторы, характеризующие ограничения по возможности реализации программ (экономический потенциал, бюджетные ограничения), состояние технологии, конструкторской проработки.

Для иллюстрации проблемы оптимизации программ вооружения будем полагать, что актуальными являются следующие задачи Вооруженных сил РФ:

- стратегическое сдерживание, включая задачи противовоздушной и противоракетной обороны;
- локализация конфликтов на континентальных театрах боевых действий;
- локализация конфликтов на морских (океанских) театрах боевых действий;
- миротворческие операции.

В табл. 2 представлено возможное задействование ресурсов для решения определенных задач по преодолению сопротивления противника в различных условиях.

Участники выполнения боевых задач и реализации программ развития ВВСТ (организационные структуры): Ракетные войска стратегического назначения (РВСН), Воздушно-космические силы (ВКС), Военно-морской флот (ВМФ), Силы общего назначения (СОН) и др. Выполнение задач может быть возложено на различные организационные структуры, например, РВСН, ВКС, ВМФ и др. (см. табл. 2). Различают программы боевой задачи и программы организационных структур. Оптимизация этих программ проводится путем распределения задач, а в

последующем – финансовых ресурсов по организационным структурам, осуществляемая на основе военно-экономического анализа, что позволяет находить наиболее эффективные решения выполнения боевых задач.

Таблица 2

Матрица оптимизации программы ВВСТ [47]

Организационные структуры	Ударные (оборонительные) стратегические средства	Космические средства	Средства борьбы на континентальных ТВД	Средства борьбы на океанских (морских) ТВД	Миротворчество
РВСН	+	+	+	+	–
ВКС	+	+	+	+	–
ВМФ	+	–	+	+	–
СОН	–	–	+	–	+

Экономика производства вооружения, военной и специальной техники базируется на следующих принципах:

- активное использование программно-целевого планирования развития систем оружия, сочетание при этом целей и задач войск с располагаемыми ресурсами;
- конкурсная основа определения разработчиков и производителей оружия, контрактные отношения заказчиков и производителей оружия;
- единство военно-технической политики для всех войск, позволяющее исключить дублирование и многотипажность создания оружия.

Военно-финансовая система всех войск должна быть единой и унифицированной. Финансирование войск должно быть построено преимущественно по территориальному принципу с использованием полевых учреждений Банка России в соответствии с Концепцией военного строительства для всех родов войск и предприятий оборонной промышленности [47].

Эффективность оборонного потенциала [48]. Качество и количество находящихся в войсках финансовых, материальных и людских ресурсов, методы и механизмы организации деятельности реализуются в процессах функционирования военной организации государства, которое, обычно, оценивается уровнем боеготовности войсковых подразделений, эффективности систем оружия, величиной их оборонного и боевого потенциалов и др. При этом по разным причинам трактовка сущности используемых показателей бывает зачастую недостаточно четкой. Так, в научной литературе оборонный потенциал определяется как совокупность материальных и духовных факторов, а сам потенциал интерпретируется как совокупность

материальных и духовных сил [49, 50]. Синонимом термина «потенциал» считается слово «возможности», а боевые возможности трактуются как «количественные и качественные показатели». Боевая эффективность определяется как степень пригодности вооружения, военной и специальной техники (ВВСТ) для решения боевых задач и уточняется, что она является одной их характеристик оружия. Можно сказать, что показатель боевой эффективности позволяет оценивать не только эффективность ВВСТ, но и действий войск [51].

Множество понятий (боевые возможности, боевой потенциал, боеспособность, боевая эффективность, боевая готовность и др.) и наблюдаемая противоречивость их определений усложняют проведение научных военно-экономических исследований и подготовку практических рекомендаций. Поэтому необходимо выявить основополагающие понятия и однозначно определить их сущность.

Экономическое содержание оборонного потенциала и боевой готовности войск. Применительно к войскам результативность их деятельности может быть описана двумя группами понятий и соответствующими им показателями, отражающими количественную и качественную стороны.

Первая группа понятий должна характеризовать наличие и качество ресурсов, имеющихся в войсках. Наиболее полно этой группе понятий соответствует боевой потенциал, который зависит от уровня оснащенности армии и флота военной техникой и укомплектованности частей, соединений и объединений кадрами военных специалистов необходимой квалификации, состояния их морального духа. Уровень боевого потенциала может измеряться суммарной мощностью огневого залпа, количеством единиц и систем оружия или степенью укомплектованности данного войскового формирования до полного штата. Однако наличие материальных и людских ресурсов не полностью характеризует возможность войсковых формирований выполнять стоящие перед ними боевые задачи. Необходимы характеристики способности войск в установленное время, во-первых, полностью реализовать имеющийся потенциал, во-вторых, увеличить боевой потенциал до размеров, необходимых и достаточных для решения боевых задач.

Вторая группа понятий характеризует мобилизационную способность экономической системы. Первая и вторая характеристика должна измеряться временными показателями. Содержанию первой из них наиболее полно соответствует понятие боевой готовности, второй – мобилизационной готовности.

Временные показатели мобилизационной и боевой готовности войск могут иметь две разновидности. Они могут либо измеряться временем перехода из одного состояния готовности в другое, либо вероятностью этого перехода за установленное время. Интегрирующим понятием следует считать боевую эффективность, ха-

рактеризующую степень приспособленности военной техники и войск в целом к выполнению боевых задач. Показатели боевой эффективности должны оцениваться величиной ущерба, наносимого противнику войсками в заданное время при определенных затратах материальных средств. Численное значение показателей в такой трактовке должно зависеть от наличия и качества материальных ресурсов, имеющихся в войсках, а также количества личного состава, уровня его специальной подготовки, полевой (морской) выучки и морального духа. Уровень боевого потенциала характеризуется объемом материальных и людских ресурсов, имеющихся в войсках, и их качеством (уровнем тактико-технических характеристик) и является величиной динамичной, изменяющейся под воздействием двух групп факторов: внешних и внутренних. Внешние факторы определяют степень угрозы для нашей страны со стороны вероятных противников, характер стоящих перед вооруженными силами боевых задач, и, следовательно, требования к количеству и качеству необходимой военной техники и численности войск. Внутренние факторы определяются уровнем развития экономического и военно-экономического потенциала государства. Следовательно, внешние факторы предъявляют требования к боевому потенциалу вооруженных сил, а внутренние – характеризуют возможности удовлетворения этих требований. При наличии определенного уровня технического оснащения войск и тактико-технических характеристик ВВСТ боевая готовность будет определяться, главным образом, обученностью личного состава. Именно она влияет на способность войск начинать боевые действия или переходить с одного уровня готовности к другому, более высокому. Наличие расчетных графиков или таблиц, разработка которых является прерогативой высшего военного руководства страны, позволяет определять моменты перехода от одного состояния боевой готовности к другой, рассчитывать длительность периода, который будет отведен войскам различных видов вооруженных сил для перехода от одного состояния к другому, предъявлять требования к содержанию боевой подготовки войск, основная задача которой состоит в том, чтобы достичь уровня обученности личного состава и состояния ВВСТ, при котором в заданное время они смогут перейти к новому состоянию готовности и выполнить боевые задачи. Боевая подготовка представляет собой совокупность мероприятий по обучению личного состава и сопровождается расходованием разнородных ресурсов. Следовательно, процесс боевой подготовки носит экономический характер. Кроме того, изменение степени боевой готовности может сопровождаться мобилизационным развертыванием, увеличением технической оснащенности войск и количества личного состава, а следовательно, повышением боевого потенциала. Изменение боевого потенциала также всегда является экономическим процессом. Но изменение уровня боевого потенциала в

экономическом смысле носит иной характер, чем текущий процесс боевой и политической подготовки войск, поскольку иными являются потребляемые при этом ресурсы и источники их удовлетворения. Если повышение боевого потенциала обеспечивается заблаговременной разработкой вооружения с требуемыми тактико-техническими характеристиками, поставками в войска материальных средств, то в ходе боевой подготовки затрачивается ресурс имеющейся в войсках техники, расходуются материалы, энергетические запасы. Следовательно, повышение боевого потенциала сопровождается наращиванием материальных ресурсов в войсках, а повышение боевой готовности требует их расходования. В этом состоит основное различие экономического содержания боевого потенциала и боевой готовности. Таким образом, оснащение войск ВВСТ и укомплектование их личным составом воздействует на изменение боевого потенциала, а боевая подготовка имеет целью освоение новой техники, обучение личного состава и, в конечном счете, повышение уровня боевой готовности войск, их способности переходить от одного состояния к другому, более высокому, и выполнять поставленные боевые задачи [52]. Боевая подготовка в своей основе содержит комплекс мероприятий по обучению и воспитанию личного состава и слаживанию подразделений, частей и соединений. Поскольку проведение мероприятий по боевой подготовке, содержанию и обслуживанию техники требуют расходования разнородных материальных ресурсов, финансирование которых осуществляется на различных уровнях распорядителей кредитов, а также расходования денежных средств по различным статьям сметы Министерства обороны, следует констатировать, что прогнозирование потребных затрат на осуществление отдельных мероприятий и учет фактически произведенных затрат представляет значительную методическую трудность [53, 54]. Если подходить к учету затрат только с позиций перечня подразделений сметы Министерства обороны, то анализ показывает, что расходы денежных средств военного округа на боевую, оперативную и физическую подготовку составляют лишь около одного процента. Разумеется, это не соответствует реальным затратам на обучение войск, так как при этом не учитывается расход моторесурса и ресурса боевой техники, амортизации зданий и сооружений, расход горючего и многое другое, что необходимо для осуществления мероприятий по боевой подготовке.

Подходы к оценке результативности военно-ориентированных мероприятий. Анализ целевой направленности мероприятий войсковой сферы деятельности по выполнению планов боевой подготовки и направлений расходов денежных средств по сметным подразделениям показывает, что существующая практика планирования и учета затрат не полностью приспособлена для проведения военно-экономического анализа мероприятий, обеспечивающих создание боевого потен-

циала вооруженных сил и повышение их боевой готовности, что существенно затрудняет исследования и подготовку рекомендаций по повышению эффективности использования военно-экономических ресурсов. Целесообразна разработка единой системы методического обеспечения планирования мероприятий, оценки размера потребляемых ресурсов (вне зависимости от источника финансирования) и достигаемых результатов боевой и политической подготовки войск.

Методическое разрешение данной проблемы представляется посредством использования программно-целевого подхода к моделированию процессов деятельности военной промышленности и структурных элементов войск. В настоящее время практически отсутствуют методики, позволяющие на единой основе систематизировать отчетные данные по каждому мероприятию, а также сравнительно оценивать полученные результаты при произведенных затратах. Тем более необходимы такого рода методики на предплановой стадии, позволяющие прогнозировать значения показателей, которые должны быть достигнуты в результате осуществления того или иного мероприятия и затраты всех видов расходуемых ресурсов. При этом методики должны предусматривать учет факторов, влияющих как на затраты, так и на результаты деятельности. Варьирование факторами позволяет выбрать оптимальный в экономическом смысле план деятельности, выполнять задачи боевой и политической подготовки с наименьшими затратами. Именно здесь находится ключ к повышению обоснованности планов и повышению эффективности планируемых мероприятий, что дает основание считать особенно важной проблему разработки комплекса методик оценки затрат и результатов по всем мероприятиям, планируемым к проведению в войсковой сфере.

Для решения данной проблемы необходимо приспособить систему оценок и учета затрат к решению целевых задач, лежащих в основе мероприятий. Система оценок результатов деятельности по отдельным мероприятиям нуждается в совершенствовании, в отходе от традиционных баллов (отлично, хорошо и т.д.), которые не характеризуют истинный уровень боевого потенциала и боевой готовности войсковых формирований. Необходимы показатели качества достигнутых результатов с учетом важности, «веса» данного мероприятия в интегральном показателе вышестоящего структурного элемента. Наиболее конструктивным представляется предложение о введении вероятностных характеристик в совокупности с «весовыми» показателями, имеющими смысл потенциалов отдельных мероприятий или структурных элементов.

Система учета затрат также требует совершенствования. Здесь главная задача состоит в том, чтобы адаптировать учет фактических затрат материальных ресурсов и денежных средств к реализации целевого принципа. Затраты должны раз-

носиться по своеобразным лицевым счетам, открываемым на каждое мероприятие. Накопление статистических данных позволит осуществить разработку методик прогнозирования затрат на все мероприятия. При этом методики оценки результатов и затрат должны предусматривать учет одних и тех же факторов. Например, методики оценки затрат на обучение личного состава должны обязательно реагировать на план обучения, сопровождающегося затратами ресурса учебной и боевой техники, расхода материальных ресурсов (горючего, электроэнергии и др.), денежных средств (включая денежное довольствие обучающих). Значит, в качестве фактора будет выступать план обучения личного состава, т.е. перечень и последовательность обучения с помощью различных учебно-тренировочных средств, что, в конечном счете, определяет достаточный уровень обученности. Выбор оптимального плана обучения в данном случае является основой для утверждения о том, что данное решение является наиболее экономичным или эффективным.

Выполнение работ по созданию комплекса методик для всех мероприятий, проводимых в войсках, является трудоемкой задачей, требующей привлечение ряда научно-исследовательских организаций и практических работников. Необходимо установление приоритетности создания методик по мероприятиям и структурным элементам. Приоритетность должна учитывать два фактора: важность того или иного мероприятия или структурного элемента с точки зрения его влияния на формирование боевого потенциала и боевой готовности войск, а также его вес в структуре затрат. Можно утверждать, что наиболее важными мероприятиями, проводящимися в вооруженных силах, являются войсковые учения и обучение личного состава с использованием учебно-тренировочных средств. Одновременно необходимо учитывать вклад отдельных структурных элементов в создание потенциала вышестоящего войскового формирования. Здесь следует исходить из того, что каждый из них может быть оценен своим потенциалом, который позволяет определить долю различных воинских частей, соединений и т.д. в интегральном показателе боевого потенциала вышестоящего структурного элемента войск. Одновременно следует провести анализ структуры затрат, позволяющий выявить наиболее ресурсоемкие этапы и виды работ. Анализ фактических расходов показывает следующее. Во-первых, структура затрат существенно меняется в зависимости от вида военной техники и расчетного количества соединений. Во-вторых, доля затрат на эксплуатацию мало изменяется в зависимости от расчетного количества соединений. В-третьих, удельный вес затрат на эксплуатацию существенно уменьшается по мере повышения сложности военной техники. В-четвертых, изменение структуры затрат зависит от учета расходов на содержание личного состава [55]. В целом можно сделать вывод, что затраты на обеспечение эксплуатации военной техники суще-

ственно значимы и требуют тщательного военно-экономического анализа и выработки рекомендаций по повышению эффективности мероприятий направленных на обеспечение и повышение боевого потенциала и боевой готовности войск. Методология оценки эффективности различных видов военно-экономической деятельности. Повышение эффективности деятельности обусловлено, прежде всего, предупреждением потерь ресурсов, используемых при достижении поставленной цели. Предупредить потери можно, лишь организуя деятельность оптимальным образом, для поиска которого следует сформировать несколько вариантов достижения цели, сравнить их и выбрать наилучший из них. Термины «цель» и «задача» употребляются главным образом по отношению к будущим действиям, предстоящим мероприятиям. Если же действие произошло или происходит, то следует употреблять термины «эффект» или «результат». Таким образом, цель и задачи преобразуются в эффект (результат) вследствие целенаправленной деятельности.

Модель процесса функционирования системы представим следующим образом. Пусть система в начальный момент времени находится в некотором состоянии S_0 и начинает функционирование во внешних условиях $\{y_{t0}\}$, решая совокупность задач $\{z_{t0}\}$. В процессе функционирования за период T происходит осуществление комплекса мероприятий, сопровождающихся потреблением разнородных ресурсов $\{C\}$, и достигается определенный результат $\{W_{ti}\}$, а система переходит в состояние S_i. Для оценки эффективности функционирования системы следует сопоставить достигнутые результаты $\{W_{ti}\}$ с произведенными затратами $\{C\}$ за период T. На этапе планирования оценка эффективности носит прогнозный характер и служит выбору оптимального варианта достижения целей деятельности. После истечения периода T оценка эффективности является мерой оптимальности ее перевода из начального состояния S_0 в состояние S_i и служит поиску резервов при последующем планировании. В реальной действительности системы состоят из ряда структурных элементов, функционально соподчиненных и организующих свою деятельность в интересах конечной цели, конечного результата. При этом результат деятельности некоторых структурных элементов носит обеспечивающий характер и полностью или частично воплощается в результате деятельности других основных элементов. Применительно к деятельности войсковых структурных звеньев может быть установлена связь эффекта, ресурсов и эффективности, достигаемой в результате осуществления мероприятий. Структурные звенья различного функционального назначения осуществляют мероприятия по боевой и политической подготовке, обслуживанию военной техники и осуществлению боевого, специального технического и тылового обеспечения. Каждое мероприятие позволяет получить

непосредственные результаты, сопоставление которых с объемом израсходованных ресурсов позволяет оценить эффективность мероприятия.

Непосредственные результаты отдельных мероприятий W_1, W_2, ..., W_k образуют общий эффект W, конечный результат деятельности данного структурного звена (соединения, объединения и т.д.). Соотношение конечного результата W с общими затратами ресурсов C позволяет оценить суммарную эффективность деятельности системы в целом. Логично считать, что экономический эффект может быть положительным или отрицательным. Так, убыток можно считать отрицательной прибылью; растраты, утраты и хищения тоже являются отрицательным результатом деятельности; эффект от модернизации образца военной техники также может быть отрицательным. С определенной долей условности можно оценивать экономический эффект применительно к боевым действиям войск. Такая оценка экономического эффекта может иметь несколько аспектов. Один из них состоит в том, что, поскольку выполнение огневых и боевых задач сопровождается расходом ресурсов (ракет, снарядов, износом военной техники и др.) и имеет свою стоимостную оценку, то используя различные варианты назначения боевых средств по целям противника, можно выполнять одну и ту же задачу с разными затратами. Следовательно, разность затрат на выполнение задачи оптимальным способом и любым другим, отличающимся от оптимального, дает определенную величину экономического эффекта. Деятельность (боевая подготовка, хозяйственная деятельность, боевые действия и др.)

Эффект следует расценивать как результат деятельности безотносительно к тому, какими усилиями он достигнут. Однако сам по себе эффект, характеризуя полученный результат, не является мерой качества деятельности по его достижению. Необходимо соотнесение результата с теми усилиями, которые будут необходимы (для планируемых мероприятий) или произведены (для осуществленных мероприятий) в интересах достижения поставленной цели. Обычно в практике исследований и при анализе результатов деятельности под эффективностью также понимается соотнесение результата и затрат. Следует заметить, что во всех трактовках понятия эффективности не учитывается фактор времени, играющий весьма существенную роль в экономических процессах и при обосновании управленческих решений. Особенно велика роль фактора времени в военном деле. Проявление фактора времени при оценке эффективности многообразно. Рассмотрим четыре основные формы его проявления.

1. При обосновании плана проведения мероприятия может оказаться, что два или более варианта позволяют получить один и тот же результат при одинаковых затратах, но за разное время. При классической оценке по критерию «затраты –

эффект» эти варианты будут равнозначными. В действительности же предпочтение следует отдать варианту, позволяющему достичь цели за более короткий срок. Могут оказаться все анализируемые варианты достижения цели непригодными, если оно происходит за рамками установленных сроков.

2. Создание сложных комплексов военной техники, строительство учебно-материальной базы войск и других объектов может осуществляться в условиях фиксированных сроков получения конечного результата, но при разных способах выполнения мероприятий, при различных темпах потребления материальных, трудовых и финансовых ресурсов. Если при этом достигается конечная цель в установленный срок, то более целесообразным следует считать тот вариант, при котором ресурсы потребляются позже. Для учета фактора времени в такого рода задачах обычно осуществляется приведение разновременных затрат к одному моменту времени.

3. В условиях современной динамичности факторов, влияющих на формирование боевых задач вооруженных сил, приоритетными будут такие системы ВВСТ, которые позволяют производить их модернизацию и развертывание в короткие сроки. Поэтому даже равноэффективные в боевом отношении и одинаковые по стоимости системы будут неэквивалентными, если они по степени индустриализации монтажно-сборочных работ, степени приспособленности к дальнейшей модернизации в возможно более короткие сроки и другим временным параметрам будут существенно отличаться друг от друга.

4. При оценке экономической эффективности обычно учитываются только дополнительные капитальные вложения. Такой подход, предполагающий учет только предстоящих затрат, ставит в предпочтительные условия те системы, которые используют при получении требуемого эффекта большие затраты прошлого труда. Поэтому методические подходы к оценке эффективности должны учитывать объективно существующую инерционность экономических процессов, наличие временного лага между затратами и проявлениями их в результативности деятельности.

Таким образом, оценка эффективности должна производиться не только по критерию «затраты–эффект», но и с учетом всех проявлений фактора времени. В наиболее общем виде критерий эффективности можно выразить триадой «затраты–эффект–время». Формулирование и расчет показателей, характеризующих временной, затратный и результатный компоненты комплексного критерия «затраты–эффект–время», связаны со значительными методическими трудностями. Кроме того, существенные помехи расчету показателей эффективности создают факторы

организационного характера, условия режима секретности, несовершенство системы сбора и хранения информации.

Интегральный показатель оценки эффективности использования военно-экономических ресурсов. Решению проблемы формулирования отдельных составляющих комплексного критерия эффективности оборонных расходов на различных уровнях (народное хозяйство – военная экономика – вооруженные силы и т.д.) посвящен ряд работ военных экономистов [56, 57]. Наибольшее внимание в опубликованных работах уделено критериям верхнего уровня. С их помощью делается попытка оценить эффективность оборонных расходов ресурсов государства и функционирования военной экономики в целом. Для решения частных задач представляется целесообразным производить оценку локальных показателей, характеризующих эффективность деятельности по отдельным направлениям использования военно-экономических ресурсов и по уровням решения задач создания и укрепления боевого потенциала и повышения боевой готовности вооруженных сил. Задачи, решаемые в интересах единой цели – повышения эффективности использования военно-экономических ресурсов, следует разделить на три основные класса: в отраслях народного хозяйства, включая оборонные отрасли промышленности; в вооруженных силах; во вневойсковом обеспечении обороны страны. В методических подходах к оценке эффективности деятельности предприятий и научно-производственных объединений, запятых созданием ВВСТ, много общего с подходами, используемыми в общепромышленных министерствах. Специфика определения экономической эффективности деятельности научно-исследовательских и опытно-конструкторских организаций и предприятий оборонной промышленности учитывается в методических разработках, выполняемых соответствующими министерствами. При этом следует учитывать, что определенная специфика характерна не для всего военного производства, а только для первого функционального сектора, где осуществляется создание конечного военного продукта. Суть специфики деятельности оборонных отраслей по созданию военной техники с позиции оценки эффективности затрат на оборону состоит в следующем:

- исследования и разработки в области военной техники и ее серийное производство происходят в условиях постоянного соперничества с вероятным противником;
- работы по созданию материальных ресурсов для вооруженных сил имеют важное государственное значение. От количества и качества ресурсов, соблюдения сроков их поставки зависит обороноспособность страны;
- сведения о состоянии и путях совершенствовании военной техники являются объектом иностранных разведок;

- для повышения уровня живучести военной экономики необходимо рассредоточение научно-экспериментальной и производственной базы промышленности;
- сроки создания новых ВВСТ определяются, как правило, динамикой внешней угрозы, что обусловливает необходимость сокращения времени на проведение научно-исследовательских и опытно-конструкторских работ, совмещения ряда этапов, неоптимальность их организации, а следовательно, вызывает повышение стоимости их осуществления:
- натурные испытания ряда образцов военной техники либо невозможны, например, проведение пусков ракет по объектам вероятного противника, либо их проведение запрещено международными соглашениями (например, наземные ядерные взрывы);
- условия режима секретности делают практически невозможным использование результатов исследований в области военной техники, проводимых вероятным противником;
- наличие института военных представительств в оборонной промышленности позволяет обеспечить требуемый уровень качества ВВСТ, но в свою очередь сопровождается значительным расходом денежных средств.

Таковы основные специфические условия деятельности оборонных отраслей промышленности, накладывающие свой отпечаток на эффективность затрат в сфере производства материальных ресурсов для вооруженных сил.

В войсковой сфере деятельности задача повышения эффективности использования военно-экономических ресурсов формулируется следующим образом: имеющиеся в войсках материальные, людские и финансовые ресурсы должны быть использованы таким образом, чтобы обеспечить требуемый уровень боевого потенциала и боевой готовности воинских частей, соединений и объединений.

Оптимизация деятельности войск, являющихся многоуровневой иерархической системой, должна осуществляться по принципу: деятельность каждого структурного элемента войскового звена вооруженных сил в мирное время должна обеспечить максимальный уровень боевой готовности вышестоящего структурного элемента в условиях ведения боевых действий. Следовательно, на каждом уровне иерархической структуры вооруженных сил не обязательно добиваться максимального эффекта. Важно, чтобы планируемый и достигаемый результат на каждом уровне обеспечивал получение максимального уровня эффективности вышестоящего звена войсковой структуры при решении боевых задач.

Важной и трудной методической проблемой является формирование и оценка результатного показателя, входящего в комплексный критерий оценки эффективности использования военно-экономических ресурсов. В настоящее время

весьма распространенной является балльная система оценок результатов боевой подготовки, финансово-хозяйственной деятельности частей, соединений и объединений, учреждений и организаций. Доступность и простота балльной оценки делает ее универсальной для структурных элементов вооруженных сил разного уровня и характера деятельности. Эта универсальность является, с одной стороны, достоинством, с другой – недостатком, поскольку разномасштабные структурные элементы потребляют существенно различные объемы ресурсов, но могут иметь одинаковый выходной результат, оцениваемый баллом.

Есть и еще один принципиальный недостаток балльной системы оценки. Результат оценивается строго дискретной величиной, принимающей всего четыре значения (отлично, хорошо, удовлетворительно, неудовлетворительно). В то же время затратная составляющая является, по существу, непрерывной величиной. Следовательно, крайне желательно, чтобы результатный показатель для любого вида деятельности был как бы объемным, отражающим масштаб структурного звена и осуществляемого им мероприятии.

Один из подходов к выработке глобального критерия эффективности расходов на оборону может состоять в следующем. Поскольку оценка эффективности предполагает сопоставление эффекта и затрат, необходимо сформулировать целевую и затратную составляющие критерия. Военная доктрина государства имеет оборонительный характер. Поэтому цель функционирования вооруженных сил может считаться достигнутой, если в течение достаточно длительного периода обеспечивается мирная жизнь нашей страны. Следовательно, результатная составляющая критерия эффективности может считаться вполне определенной и достигнутой. Тогда вторая (экономическая) составляющая может быть представлена показателями национального дохода, что обусловлено корреляционной связью между размером оборонных расходов и народнохозяйственной эффективностью. Это позволяет связать эффективность военной экономики с эффективностью экономики страны в целом [58]. В качестве результатной составляющей показателя эффективности для вооруженных сил в целом может быть принята величина, имеющая относительный характер – степень соответствия достигнутого уровня боевого потенциала вооруженных сил, требуемому для выполнения стоящих перед ними задач. Для отдельных образцов вооружения может рассчитываться, например, количество боеприпасов, необходимых для выполнения боевой (огневой) задачи, поражаемая площадь в полосе обороны противника, количество уничтожаемых объектов. Однако, чем выше уровень агрегирования средств вооруженной борьбы и войсковых формирований (соединение – объединение – вид вооруженных сил), тем труднее выразить показатель боевой мощи войск числом, не являющимся относительной

величиной. Тем более это справедливо для вооруженных сил в целом. В то же время относительная величина, характеризующая готовность вооруженных сил к выполнению стоящих перед ними задач, имеет свой недостаток при использовании его для оценки эффективности. Это связано с тем, что объем боевых задач, стоящих перед вооруженными силами, не является постоянным. Увеличение объема решаемых задач обусловлено изменением количества объектов поражения их защищенности, усилением средств противодействия. Поэтому степень готовности вооруженных сил, будучи даже постоянной относительной величиной потенциально различна в различные годы. Целесообразно вести показатель, характеризующий темп роста боевых возможностей вооруженных сил в динамике, приняв за единицу уровень определенного года. Затратная составляющая показателя эффективности в этом случае должна рассчитываться путем суммирования расходов на оборону за этот же период. Отношение суммарных расходов государства за расчетный период к индексу боевого потенциала вооруженных сил, достигнутого к концу расчетного периода, может характеризовать тенденцию показателя эффективности оборонных затрат и функционирований военной экономики в целом. Весьма ощутимую роль в повышении эффективности затрат ресурсов в вооруженных силах принадлежит штабам всех уровней. Эффективность их деятельности следует оценивать с позиций оптимальности внутренней организации и с позиций эффективности деятельности подчиненных войсковых формирований, которая является определяющей и характеризует конечную цель деятельности штабов как органов управления.

Органы управления войсками реализуют различные функции, качество осуществления которых в решающей мере влияет на эффективность деятельности управляемых войсковых формирований. Эти функции состоят в обосновании планов боевой подготовки, перспектив развития систем военной техники, заказов вооружения в промышленности, обеспечении поставок материальных ресурсов, организации проведения научных исследований в вооруженных силах и координации научных исследований в оборонной промышленности. Существенную роль в укреплении боевого потенциала вооруженных сил и повышении эффективности затрат ресурсов на оборону страны и грает система вневойскового обеспечения. Главными задачами этой системы является подготовка кадров для вооруженных сил и создание материальной базы повышения живучести военной экономики. В эту систему входят военные комиссариаты, военно-спортивные организации и органы гражданской обороны. Эффект деятельности учреждений вневойсковой подготовки личного состава проявляется в уровне обученности призывников и офицеров запаса, приходящих в войска по призыву и мобилизации. Чем выше уровень первоначальной подготовки кадров

армии и флота, тем быстрее они достигают требуемого уровня обученности, и тем выше показатели боевой готовности войск.

2.3. Организация экономической защиты системы

Антикризисные мероприятия. Обострение международной обстановки неминуемо сказывается на конъюнктуре товарных, сырьевых и финансовых рынков. Как правило, наблюдается рост цен на стратегическое сырье и материалы, а на фондовых рынках отмечается стремительное падение биржевых индексов, обесценивание ценных бумаг корпораций и иные негативные явления. Кризис в международных отношениях неминуемо влечет за собой и финансово-экономический. В середине прошлого века была сформирована международная финансово-экономическая рыночная среда, одной из характеристик которой стало появление глобальных кризисных процессов [59]. Из-за экономических и финансовых кризисов уменьшается национальный доход государства и наблюдаются безработица и банкротства, что значительно ухудшает условия жизни населения даже развитых стран. Как правило, кризисы растягиваются в депрессионную фазу, которая продолжается достаточно длительное время. Она замедляет экономический рост и тормозит научно-технический прогресс. Глобальный кризис 2008–2009 гг. и последующая многолетняя рецессия позволили выявить основные причины формирования финансовых кризисов. Устранить и нейтрализовать их оказалось возможным только совместными и скоординированными действиями многих стран, а также путем ускоренного перехода к новому инновационному технологическому укладу. Имеющиеся показатели экономической статистики убедительно подтверждают, что современные кризисы становятся более длительными и глубокими. Это обстоятельство заставляет разрабатывать и практически применять прогрессивные методы и механизмы, препятствующие их появлению. В период кризиса совершенствуются, расширяются и заметно усиливаются эффективные действия разнообразных антикризисных механизмов [60]. Их использование позволяет снизить негативные последствия резкого снижения промышленного производства и защитить национальные рынки.

Для борьбы с кризисными процессами многие ведущие страны мира разрабатывают и практически реализуют стратегические антикризисные планы [61]. Так, например, в соответствие со стратегическим планом США во многих американских штатах были созданы антикризисные механизмы, предназначенные для развития инфраструктуры, поддержки жилищного строительства с ипотеки. Во время кризиса 2008–2009 гг. Сенатом и Конгрессом США был одобрен почти 1000-страничный

план по стимулированию и инновационному развитию американской экономики. На его финансирование было выделено в 787 млрд долл. Большая часть разработанного плана была связана с развитием рынка недвижимости. В плане предлагались эффективные методы решения проблем ипотечного финансирования, повышения доступности жилья, обновления инфраструктуры, развития проектов, связанных с альтернативной энергетикой и территориальным развитием. В период кризиса Федеральная резервная система США осуществила практическую реализацию программы выкупа ценных бумаг и прямых обязательств ипотечных брокеров, на выполнение которой предусматривался один год. Для поддержки рынка недвижимости планом вводилось запрещение отчуждения жилых домов, облегчение бремени выплат для ипотечных заемщиков, стабилизация балансов финансовых институтов и стимулирование выдачи новых кредитов. Американские граждане получили возможность переоформить свои кредиты на более дешевые с уменьшенными процентными ставками. План поддержки предполагал также, что выдававший кредит банк добровольно снизит кредитные ставки для заемщиков, которым угрожает отчуждение жилья. При этом правительство было обязано выплатить банку финансовое вознаграждение за каждый переоформленный ипотечный договор. В плане имелась и законодательная инициатива. Она позволяла судам, введении которых были дела заемщиков и владельцев, имеющих единственное жилье и ставших неплатежеспособными, пересматривать условия ипотеки. В процессе принятия решений судьи могли увеличивать временной период кредитования, уменьшать процентные ставки, а также основную величину долга приводить в соответствие со «справедливой» ценой жилья. Антикризисный план также способствовал предотвращению роста процентных ставок по кредитам и стимулированию крупных финансовых организаций к оформлению новых кредитов для приобретения гражданами жилых помещений. Для успешного достижения этой цели банки были дополнительно профинансированы.

Антикризисные планы экономически развитых государств предусматривали выделение значительных финансовых средств на развитие транспортной инфраструктуры, физический износ которой во многих странах был достаточно высок. В этих планах одним из главных стратегических направлений стало дальнейшее развитие системы скоростных магистралей. На это направление были предусмотрены значительные финансовые ресурсы из государственного бюджета. Правительства многих стран выделяют миллиарды долларов на создание в них высокоскоростных железнодорожных систем и комплексов, а также современных грузовых и пассажирских интермодальных терминалов. Такие терминалы способны выполнять комбинированные транспортировки и обладают синергетическим эффектом, возникающим

от совмещения на одном транспортном пункте автомобильных, авиационных и железнодорожных грузовых и пассажирских потоков. Такой новый транспортный центр построен, в частности, в Майами. В США на рынок недвижимости непосредственно было выделено около 2% от общих расходов антикризисного плана. Большая часть этих средств распределяется между конкретными региональными проектами. Остальные средства направляются на поддержку проектов по энергосбережению и на реализацию программ снижения и устранения негативного воздействия различных дестабилизирующих эффектов. Принятый Конгрессом США план стимулирования экономики страны – это не только план борьбы с кризисом, но и своеобразный мост в будущее. Действительно, технологии XIX и XX вв. уже не работали, а железные дороги, построенные в середине XX в., должны быть заменены на более эффективные и современные. То же самое относится и к средствам передачи информации и электроэнергии. При этом указываются новые источники энергии – ветер, солнце и т.п. Также план предоставлял лучшие возможности для образования всех слоев населения с тем, чтобы поддерживать конкурентоспособность США в будущем. Чтобы вернуть людям работу и в то же время уменьшить зависимость от импортных поставок нефти, планом предлагалось вложить финансовые средства в производство возобновляемых энергоресурсов и модернизацию общественных зданий. На эти цели было выделено 35 млрд долл. На науку и передовые технологии было выделено еще 22 млрд долл. Перестройка дорог обошлась американцам в 22 млрд долл. Еще 20 млрд долл. было потрачено на решение экологических проблем. Расходы на образование в виде налоговых субсидий школам и колледжам, налоговых вычетов для граждан, финансирования многих образовательных программ составили 85,2 млрд долл. На поддержку и модернизацию медицинских учреждений было выделено 21 млрд долл. Эти средства позволили снизить цены на медицинские услуги и улучшить здоровье граждан. Тем, кто остался без работы, были предоставлены налоговые вычеты, а также возможность обучиться новой профессии и найти новую работу. Также должникам по ипотеке были предложены программы реструктуризации долгов. Другие развитые страны для противодействия кризисам также предпринимали значительные финансовые вливания в экономику. Так, в Японии объем мер по стимулированию экономики составил 110 млрд долл., а в Германии – более 70 млрд долл. Однако такое стимулирование внутреннего спроса оказалось недостаточным. Падение ВВП в этих странах было существенным: в Германии оно составило 6%, а в Японии 6,1%. Кроме того, экономическая обстановка в Германии повлияла на ситуацию во всей зоне евро. Так, прогноз снижения ВВП оказался в пределах 4,4%, а снижения производства в восточноевропейских странах еще выше. А ведь значительная доля экспорта этих предназначалась для рынка Германии. Тем не ме-

нее некоторым Восточно-европейским странам удалось привлечь в свою промышленность иностранные инвестиции. Это позволило удерживать относительно неглубокой уровень рецессии. Например, падение ВВП Польши в 2009 г. составило 0,8%, Чехии – 3%, Словакии – 5% [62].

Мировой опыт свидетельствует о том, что антикризисные инновации могут создаваться мелкими и средними компаниями, поскольку крупные структуры не склонны к риску, с которым сопряжен технологический прорыв. В США, которые считается технологическим мировым лидером, 75% новых рабочих мест создается малым и средним бизнесом, 70% открытий и изобретений приходится на их долю, 75% богатых американцев трудится в этой сфере. В России недостаточная активность некоторых научно-исследовательских центров и высших учебных заведений, которые расходуют значительную часть научного бюджета, приводит к тому, что инновационная антикризисная модернизация осуществляется медленными темпами. Научное сообщество должно повышать квалификацию своих сотрудников с помощью новых интеллектуальных образовательных систем и требовать внимания к его нуждам. Это позволит повысить престиж науки, привлечь способную молодежь к научной деятельности, результатами которой станет научное обоснование и создание новых эффективных антикризисных механизмов.

Противодействие финансово-экономическим санкциям. Важным внешним политическим фактором является санкционная политика ряда государств. С целью повлиять на определенные страны, мировым сообществом, его частью или отдельным государством, в разные годы предпринимались попытки добиться своей цели, таргетируя жизненно важные факторы производства, такие как труд, капитал, информация и бизнес. В работе «Факторный анализ внешней и внутренней среды наукоемкого предприятия на примере отечественной ракетно-космической промышленности» [63] были идентифицированы основные инструменты сдерживания развития экономических систем (табл. 3).

Во второй половине XX в. торговые войны и санкции постепенно вытесняли с мировой арены горячие конфликты. Особенно продолжительными были ограничения, введенные США против Кубы и Ирана, Северной Кореи, СССР и других стран. Жесткие санкции ЕС и США, введенные с 2014 г. против России, уже привели к ощутимым потерям для всех стран, участвующих в конфликте. Особенно болезненным для космической и других оборонных отраслей оказались ограничения в поставках ряда комплектующих и электронных приборов, используемых в ракетно-космической и авиационной промышленности, судостроении и производстве вооружений. Вместе с тем у стран, имевших ощутимый научный задел и сумевших сохранить свою производственно-промышленную базу, получилось, хотя и

с определенными проблемами, выдержать санкционное давление и добиться обнадеживающих результатов.

Таблица 3

Результат активизации факторов сдерживания [63]

Направления сдерживания	Методы сдерживания	Ожидаемый результат для инициаторов санкций	Возможный результат в стране
Труд	Введение визового режима	Осложнения при заключении международных контрактов	Возможность заключения внутренних контрактов
		Затруднение выполнения действующих контрактов	Возможность привлечения местной рабочей силы
		Осложнения туристических поездок	Развитие внутреннего туризма
	Запрет на работу в стране специалистов	Осложнения в реализации проектов	Снижение вероятности утечки информации
	Отказ в выдаче разрешений на работу мигрантам из страны	Последствия высокого уровня безработицы в стране	Предотвращение «утечки мозгов»
Капитал	Прекращение финансирования инвестиционных проектов в стране	Осложнения в реализации проектов	Снижение зависимости от иностранного капитала
	Ограничения в доступе к международному рынку ссудных капиталов (МРСК) для страны	Удорожание проектов, осложнения в их реализации	Возможность оптимизации финансирования
		Рост процентных ставок	Независимость от МРСК
		Отток капитала (валюты) из страны	
	Ограничение финансовых трансакций	Замедление оборота, снижение производительности	Создание собственного клирингового центра
	Ограничения в торговле, введение таможенных пошлин на импорт	Сокращение доли мирового рынка	Сокращение издержек производства
		Снижение конкурентоспособности страны	Повышение качества продукции
		Снижение притока валюты в страну	
		Сокращение производства в стране	
		Рост уровня безработицы	
	Ограничения на прямые инвестиции в страну	Снижение производства в стране	Снижение зависимости от иностранного капитала
		Снижение поступления валюты в страну	Снижение оттока капитала
		Снижение конкурентоспособности страны	
	Ограничения на портфельные инвестиции	Сокращение поступлений валюты в страну	Снижение зависимости от колебаний рынка

Окончание табл. 3

Направления сдерживания	Методы сдерживания	Ожидаемый результат для инициаторов санкций	Возможный результат в стране
Природные ресурсы	Управление стоимостью ресурсов спекуляциями на мировых сырьевых биржах	Влияние на развитие промышленности в стране	Диверсификация промышленности
		Искусственное «заражение» «Голландской болезнью»	
Бизнес	Запрет на международные контракты	Сокращение доли мирового рынка	Переориентация на местные рынки
		Снижение конкурентоспособности страны	
		Снижение притока валюты	
		Сокращение производства	
Информация	Запрет на доступ к технологиям	Снижение конкурентоспособности страны	Активизация внутренних научных исследований и разработок
		Сокращение производства	
	Запрет на проведение научных мероприятий	Осложнения в проведении научных исследований	
	Запрет доступа к БД		

Во второй половине XX в. торговые войны и санкции постепенно вытесняли с мировой арены горячие конфликты. Особенно продолжительными были ограничения, введенные США против Кубы и Ирана, Северной Кореи, СССР и других стран. Жесткие санкции ЕС и США, введенные с 2014 г. против России, уже привели к ощутимым потерям для всех стран, участвующих в конфликте. Особенно болезненным для космической и других оборонных отраслей оказались ограничения в поставках ряда комплектующих и электронных приборов, используемых в ракетно-космической и авиационной промышленности, судостроении и производстве вооружений. Вместе с тем у стран, имевших ощутимый научный задел и сумевших сохранить свою производственно-промышленную базу, получилось, хотя и с определенными проблемами, выдержать санкционное давление и добиться обнадеживающих результатов.

В проведенных ранее исследованиях было выявлено, что СССР находился под постоянными санкциями со стороны ведущих империалистических держав – США, Великобритании, Франции. Причем начало экономической войны против СССР совпало с началом реализации плана индустриализации страны. Так, первая пятилетка началась в 1929 г., а уже в 1930 г. санкции против СССР ввели США и Франция, а в 1933 г. к ним присоединилась и Великобритания. В послевоенный период санкции против СССР регулировались так называемым Координационным

комитетом по экспортному контролю (КОКОМ), созданным в 1949 г. для контроля за экспортом стратегических товаров и технологий в страны Варшавского договора. Основным принципом деятельности КОКОМ была реализация так называемой стратегии контролируемого технологического отставания, в соответствии с которой новые технологии, оборудование и товары могли передаваться в СССР и его союзникам не раньше, чем через 4 года после запуска их в серийное производство на Западе. Деятельность этой организации формально продолжалась до 31.03.1994. Одновременно с деятельностью КОКОМ в отношении СССР в США с 1974 г. действовала так называемая поправка Джексона-Вэника к закону о торговле, которая отменяла режим наибольшего благоприятствования в торговле и запрещала выдавать государственные кредиты и кредитные гарантии, что существенно усложняло экономические отношения между странами. Хотя с 1991 г. основания для поправки потеряли смысл, отменять ее не спешили. Более того, Конгресс США рассмотрел вопрос об отмене ограничительной в отношении России поправки Джексона-Вэника лишь в увязке с законом о введении визовых санкций против чиновников, причастных к нарушению прав человека (пресловутый закон о «списке Магнитского»). 18.07.2012 сенат США объединил эти два законопроекта в один. Интересно, что по отношению к Украине поправка Джексона-Вэника была отменена уже в 2006 г. [64].

Оценка интенсивности внешних ограничений. Для разработки стратегии экономической защиты следует оценить степень воздействия внешних ограничений на экономическую систему. На базе проведенного анализа была построена хронология введения российских санкций в период 2014–2022г., и каждое санкционное событие причислено к одному или несколькими типам санкций. Для каждого события выделены ключевые «получатели» (то есть крупнейшие российские компании и банки) для дальнейшего присваивания весов каждому событию. Это было сделано для того, чтобы более точно определить интенсивность того или иного санкционного события на долговой рынок. По нашему убеждению, ограничения на привлечение финансирования введенные, например, Австралией в адрес российских банков, будут несопоставимы по силе эффекта американским.

Для определения весов каждого события мы взяли следующие факторы:

- для определения значимости финансовых санкций w_f;
- доля санкционируемых банков в активах банковской системы России w_{bank};
- объем активов санкционируемых компаний к ВВП в текущих ценах w_{corp};
- доля валюты страны отправителя санкций в портфеле внешнего долга банков (кроме ЦБ) $w_{fcybank}$;

- доля валюты страны отправителя санкций в портфеле внешнего долга нефинансовых организаций $w_{fcycorp}$;
- для торговых санкций – доля страны отправителя санкций в общем объеме внешней торговли с Россией (по данным Comtrade) в среднем за период с 2009 по 2013 г. включительно (т.е. до начала введения санкций – w_r;
- для технологических санкций – доля страны отправителя санкций в объеме добычи трудноизвлекаемых нефти и газа (unconventional oil and gas) w_u;
- эффект санкций SDN на долговой рынок w_s является, на наш взгляд, довольно ограниченным. Санкции SDN вводились точечно, и в подавляющем большинстве в адрес конкретных физических лиц, не имеющих высокой активности на локальном и международном рынках капитала. Лишь в редких случаях санкции SDN затрагивают лиц, владеющих (прямо или косвенно) крупными российскими компаниями или банками. Такое исключение, возможно, составляют активы группы компаний VOLGA (которая, к сожалению, не раскрывает консолидированную отчетность, ограничивая возможность включения в модель), принадлежащих Г. Тимченко, активы, принадлежащие братьям Ротенбергам, и некоторые другие. Ввиду незначительности этой группы, каждому событию санкций SDN мы присвоили очень низкий вес, равный 0,1. Для определения весов финансовых санкций w_f мы воспользовались данными статистики Банка России по внешнему долгу, данными об объемах активов финансовых организаций, публикуемые Банком России, данными консолидированной финансовой отчетности (при наличии) компаний, данными International Energy Agency о добыче трудно извлекаемой нефти и газа и оценками независимых экспертов.

Индекс санкций I_τ определяется накопленным итогом путем сложения логических переменных s (1 или 0) для каждого из четырех типов санкций, взвешенных по соответствующим типам факторов, описанным ранее:

$$I_\tau = \sum_{t=1}^{T}\sum_{s=1}^{S}\sum_{r=1}^{R}\sum_{f=1}^{F}\sum_{u=1}^{U} S_{tsrfu} W_f W_r W_u W_s , \quad (1)$$

где $$W_f = \sum_{t=1}^{T}\left(W_{fcybank} W_{bank} + W_{fcybank} W_{corp}\right). \quad (2)$$

При анализе результирующих весов становится ясно, что наибольшее влияние оказывают санкции, введенные против системных российских банков, так как их доля в активах банковской системы составляет 58%.

При этом санкции против компаний нефтегазового сектора будут иметь несколько меньшее значение для долгового рынка России в целом по причине относительно небольшой (хоть и значимой) доли во внешнем финансировании. Эффект

будет заметнее в среднесрочной перспективе на объеме инвестиционных затрат на разведку и добычу нефти и газа, если предположить, что часть из них будет финансироваться за счет долга. В настоящее время значимый рост инвестиций в разведку и добычу ограничивается инициативами по сокращению добычи нефти и, естественно, динамикой цены на энергоносители. В долгосрочной перспективе наибольшие опасения вызывают санкции, связанные с ограничением на поставки в Россию высокотехнологичного оборудования для добычи нефти в Арктике, на глубоководном шельфе, а также сланцевой нефти (технологические санкции). Однако с точки зрения индекса интенсивности санкций, значимое влияние такие ограничения имеют, если они введены страной – обладателем данной технологии, а именно США и Канадой.

Модифицированный индекс санкций, на наш взгляд, более точно отражает динамику и жесткость санкционного режима в сравнении с индексом по К. Дрегеру. Данный индекс может быть использован в качестве аналога фактора «политический (санкционный) риск» при построении макроэкономической модели зависимости динамики развития долгового рынка: объем рынка, средневзвешенная стоимость долга, срок финансирования, валютная концентрация, тип долгового инструмента («внешний – внутренний»), а также от основных макроэкономических показателей:

- внешних – роста мирового/регионального ВВП, учетных ставок основных валют, динамики мирового движения капитала на развивающихся рынках, «шоков» ликвидности на мировых рынках капитала, стоимости нефти, политических (санкционных) рисков и пр.;
- внутренних – динамики российского ВВП, уровня инфляции, обменного курса, оттока капитала и пр.

Недостатком предложенной модели расчета модифицированного индекса санкций, на наш взгляд, является то, что формируемый модифицированный индекс санкций является статическим и не включает эффекта «адаптации» рынка к введенным ограничениям.

2.4. Научные исследования и разработки как элемент защиты экономической системы

Проблемы, которые сегодня определяют военную безопасность государства, выходят далеко за рамки возможностей чисто отраслевого подхода и даже экономической науки в целом. Очень многое зависит от взаимодействия экономи-

ческих и политических факторов. Кроме того, нужно учитывать ещё один важнейший фактор формирования оборонного потенциала государства − использование достижений науки и техники. Научно-технический прогресс, с одной стороны, и социально-экономическое развитие страны, и совершенствование систем обеспечения её обороноспособности − с другой, взаимно обусловливают друг друга. Таким образом, роль фундаментальных исследований в обеспечении обороноспособности страны заключается в генерации знаний, на основе которых могут быть созданы принципиально новые образцы ВВСТ, а их место – в начале программного цикла, когда в рамках очередной государственной программы формируется облик перспективной системы вооружения. В этой связи представляется целесообразным сформировать специальную программу (подпрограмму) фундаментальных, прогнозных и поисковых исследований в области обороны и безопасности страны, которая позволяла бы замкнуть цикл исследований: от программы исследований – к прикладным технологическим исследованиям, и от последних – к разработке перспективных вооружений.

Взаимосвязь между фундаментальными исследованиями и работами в области обеспечения обороноспособности осуществляется посредством механизмов, отличающихся национальной спецификой. Российский механизм использования результатов фундаментальных исследований в системе военной безопасности во многом базируется на достижениях советского периода. Военно-стратегический паритет СССР с его потенциальными противниками свидетельствует о достаточной эффективности системы организации фундаментальных исследований, действовавшей в условиях плановой экономики. Результаты фундаментальных исследований всегда являлись основой для создания новых видов ВВСТ, оснащение которыми вооружённых сил вызывало трансформацию их организационной структуры и характера военных (боевых) действий [65]. Процесс воспроизводства знаний продолжал развиваться по инерции в первые годы рыночных преобразований, но по мере их углубления начал затухать. С военно-технической точки зрения это проявилось в исчерпании накопленного ранее научно-технического и производственно-технологического потенциала в ОПК и постепенном отставании российских образцов ВВСТ от продолживших своё развитие зарубежных аналогов. В условиях усилившейся разобщённости субъектов отечественной индустрии знаний, без должной подпитки результатами фундаментальных исследований отечественные оборонные предприятия вынужденно продолжили эскалацию ранее накопленного научно-технического потенциала. Между тем, комплекс научно-практических результатов, технологий и изделий, ориентированных на создание оружия индустриальной и постиндустриальной эпохи, имеющего мощные поражающие характери-

стики, но отличающегося слабой защищённостью и автономностью, низкой избирательностью, отсутствием разнообразия в формах воздействия, а также рядом других особенностей, демонстрирующих его невысокую «интеллектуальность», исполнил свою миссию и был либо реализован в отдельных образцах ВВСТ, либо потерян в перестроечный дезинтеграционный период, когда проводилась непродуманная и слабо обоснованная государственная конверсионная политика. Исчерпание накопленного в советское время научно-технического и технологического задела привело к устойчивому снижению доли современных образцов вооружения. В итоге не только отдельные комплектующие, а целые системы вооружения для оснащения отечественных вооружённых сил начали приобретаться за рубежом, что недопустимо как с военной (низкая эффективность применения импортных образцов ВВСТ в реальных боевых действиях уже неоднократно подтверждалась практикой последних лет), так и с социально-экономической точки зрения (иностранные производители получали стимул для развития за счёт средств российских налогоплательщиков). Учитывая уже наступившие кардинальные изменения характера военных действий и, соответственно, свойств образцов ВВСТ, применение которых будет гарантировать победу, необходимо незамедлительно приступить к воссозданию инновационного отечественного научно-технического и технологического потенциала оборонных производств.

Такая стратегия обеспечит эффективное сдерживание внешней агрессии против нашей страны в условиях, когда научно-технологический прогресс делает ядерное оружие недостаточным инструментом нейтрализации таких вызовов. Нетрадиционные виды оружия (вооружения, создаваемые на основе новых физико-технических принципов), а также качественно модернизированные традиционные ВВСТ в ближайшее время могут превратиться в главную основу поддержания существующего военно-стратегического паритета. Задача осложняется тем, что в последние десятилетия фундаментальный и прикладной научно-технический задел практически не создавался в рамках государственного оборонного заказа и финансировался, как правило, по остаточному принципу [66]. Отечественное оборонное ведомство, отказываясь от проведения собственных научно-технологических исследований, в лучшем случае может рассчитывать лишь на предоставление зарубежных технологий позавчерашнего дня [67]. Подобная политика не только не способствует генерации новых научно-технологических идей учёными и специалистами Российской академии наук, сектора высшей школы и отечественной промышленности, но и грозит утратой тех позиций, по которым отечественные военные технологии могут конкурировать с зарубежными. Накопленный в советское время научно-технический и производственно-технологический потенциал настолько ве-

лик, что, даже несмотря на стагнацию индустрии знаний, отечественный ОПК продолжает оставаться высокотехнологичным сегментом отечественной экономики, занимающим ведущее место в обеспечении национальной безопасности, решении оборонных и социально-экономических задач страны. Однако и этот ресурс рано или поздно будет исчерпан. Уже сегодня Россия занимает лидирующие позиции и имеет разработки мирового уровня только в трети из 34 важных технологических направлений, а до коммерческого применения в стране доведено лишь 16% технологий, из которых мировому уровню соответствует половина. С макроэкономической точки зрения, стагнация воспроизводства знаний и обусловленный этим дефицит новых технологий чреваты нулевым ростом удельного веса организаций добывающих и обрабатывающих производств, осуществляющих технологические инновации, что и наблюдается на протяжении многих лет и приводит к снижению конкурентоспособности страны, обусловливает её неспособность встать на инновационный путь развития в условиях внешних рисков, вызванных турбулентностью мировой экономики и политической нестабильностью. Повышение эффективности использования достижений фундаментальной науки в системе ОПК России. Возобладавшая в 1990-е гг. парадигма развития российского ОПК была основана на представлении его как самостоятельном рыночном субъекте, источником развития которого является конкуренция. Эта парадигма остаётся доминирующей, что проявляется в продолжении процессов приватизации и акционирования, а также сохранении пассивной модели взаимодействия ОПК и Минобороны России как государственного заказчика ВВСТ. Во многом именно ориентация на эту модель привела к плачевному состоянию отечественных оборонных производств и обещает в будущем ещё большее снижение научно-технического и производственно-технологического потенциала ОПК, а следовательно, снижение его возможностей по созданию перспективных образцов вооружения и военной техники (это видно из постепенного вытеснения с мирового рынка российской оборонной продукции). Нужна другая, активная модель взаимодействия, причём реализующаяся на всех стадиях жизненного цикла образцов ВВСТ. Взаимодействие должно быть организовано таким образом, чтобы каждый рубль федерального бюджета, поступающий в ОПК, обеспечивал не только выполнение соответствующего государственного контракта, но и давал импульс его развитию и наращиванию конкурентных преимуществ. Используя подобную модель, можно изменить парадигму развития ОПК, обеспечив совершенствование всего комплекса технологий (промышленных, военных и т.д.). Для этого требуется ясная и чёткая военно-техническая политика, реализуемая в комплексе с промышленной политикой через программно-целевое планирование развития отечественного ОПК, которое хорошо зарекомендовало се-

бя при использовании в разработках новых систем вооружения российских армии и флота. Планирование развития ОПК осуществляется и в настоящее время. Однако мы говорим о создании системы планирования более высокого уровня, позволяющего осуществлять рациональное распределение ресурсов множества субъектов по мероприятиям в различных сферах деятельности государства и с учётом множества разнообразных факторов: процессов, проходящих в мировой и отечественной экономике и оборонно-промышленном комплексе, современных особенностей геополитического положения и военного строительства Российской Федерации, организационных преобразований системы государственного и военного управления, развития законодательной и нормативно-правовой базы национальной безопасности РФ. Методология программно-целевого планирования развития ОПК должна опираться на осознание того факта, что создание образцов вооружения и военной техники, отвечающих требованиям инновационной армии, в условиях ресурсных ограничений возможно только путём опережающего развития научно-технического и производственно-технологического потенциала российской экономики в целом и оборонно-промышленного комплекса в частности. Программно-целевое планирование развития ОПК должно осуществляться по следующим направлениям [68]:

- рациональная увязка годового, среднесрочного и долгосрочного планирования;
- реализация принципов государственно-частного партнёрства;
- усиление межпрограммной координации работ, выполняемых в соответствии с оборонноориентированными федеральными целевыми программами и государственной программой вооружения, в интересах эффективного использования финансовых ресурсов, поступающих в ОПК из различных источников;
- реализация на практике принципов бюджетирования, ориентированного на результат;
- сбалансированный учёт интересов государства и оборонных предприятий, в том числе в части распределения рисков, возникающих при выполнении государственного оборонного заказа;
- рациональное комплексирование источников развития научно-технического и производственно-технологического потенциала ОПК в интересах создания перспективных образцов ВВСТ и др.

Чтобы программно-целевое планирование стало действенным инструментом эффективного развития оборонно-промышленного комплекса, необходимо создавать механизм трансформации результатов фундаментальных исследований в факторы повышения обороноспособности Российской Федерации [69]. Функцио-

нирование этого механизма при программно-целевом планировании развития ОПК должно обеспечивать формирование функции целеполагания, причём в таком виде, который позволил бы рациональным образом совместить интересы:

- государства, отвечающего за обеспечение обороноспособности страны путём предотвращения технологического отставания от других стран, повышения конкурентоспособности отечественной экономики и перевода её на инновационный путь развития;
- государственных заказчиков, прежде всего Минобороны России, ориентированных на создание эффективных образцов ВВСТ, удовлетворяющих потребности будущих войн и обладающих таким свойством, как экономичность;
- предприятий и организаций ОПК, основная цель которых заключается в повышении собственной конкурентоспособности за счёт наращивания выпуска высокотехнологичной продукции военного и гражданского назначения, отвечающей требованиям внутреннего и мирового рынков.

Ключевым элементом механизма трансформации результатов фундаментальных исследований в факторы повышения обороноспособности Российской Федерации должна стать организационная структура, которая обеспечивает поиск результатов, имеющих высокий потенциал с точки зрения качественного улучшения продукции как военного, так и гражданского назначения, выпускаемой ОПК. Представляется, что благодаря формированию предлагаемого механизма и за счёт программно-целевого планирования развития ОПК можно будет обеспечить повышение спроса на инновационную продукцию отечественного производства, в первую очередь наукоёмкую и высокотехнологичную. Появление такой продукции невозможно без инноваций различного типа, создание которых является ключевым аспектом экономической эффективности фундаментальных исследований. Сегодня спрос на инновационную продукцию отечественного производства остаётся низким, и во многом именно поэтому повышение активности инновационной деятельности предприятий, в том числе оборонных, остаётся лишь благим пожеланием. В современных условиях нужно создавать систему, в которой именно результаты фундаментальных исследований стимулируют развитие высокотехнологичного производства. Поскольку в условиях рынка государство реально управляет только сферой обеспечения национальной безопасности, то военно-ориентированные программы и планы должны стать основой ресурсного обеспечения таких исследований. При этом необходимо руководствоваться следующими основными принципами: целеустремлённость, системность, сквозное планирование, сбалансированность, государственное регулирование деятельности организаций ОПК, согласованность федеральных и региональных интересов при приоритете государственных

интересов в решении вопросов функционирования и развития ОПК, экономичность по всем аспектам деятельности (всё должно быть нацелено на достижение результатов с минимальными затратами), прозрачность и понятность логики принимаемых в сфере фундаментальных исследований решений как для участников технического оснащения, так и для налогоплательщиков, обучаемость, позволяющая накапливать опыт и быстро адаптироваться к изменению внешних и внутренних условий функционирования, оперативность реагирования на возникновение потребностей. Направлениями организационно-экономического совершенствования механизма превращения результатов фундаментальных исследований в факторы повышения обороноспособности Российской Федерации должны стать:

- обеспечение чёткого целеполагания развития ОПК на длительный период;
- организация эффективной системы социально-экономических отношений в ОПК, стимулирующей оборонные предприятия к активизации инновационной деятельности и обеспечивающей тем самым их мотивацию к созданию передовой продукции военного и гражданского назначения;
- мобилизация всех ресурсов (инвестиционных, кадровых, информационных и т.д.), которые могут обеспечивать разностороннее развитие ОПК и непрерывность наращивания его научно-технического и производственно-технологического потенциала;
- формирование экономически эффективного механизма управления процессами создания и реализации результатов интеллектуальной деятельности, который способствовал бы возникновению единого информационно-технологического пространства ОПК, позволяющего эффективно воспроизводить и распространять знания, получаемые при выполнении работ оборонной направленности, между оборонными предприятиями в интересах создания конкурентоспособной продукции военного и гражданского назначения, а также снижению затрат на выполнение новых НИОКР за счёт повышения уровня информированности об имеющихся разработках.

Цикл разработки и производства ВВСТ – фундаментальная наука, прикладная наука, НИОКР, освоение, внедрение – в России сегодня фактически разорван, разрушено единство финансирования и управления фундаментальной наукой. Основная причина – «модернизация» механизмов её функционирования. Реформы отрицательно сказались на академической науке, поставив её на грань выживания. Отраслевая ведомственная наука, на которой держался процесс разработки новых ВВСТ, ликвидирована, корпоративная наука до сих пор не создала достойного аналога. Поэтому выстроить надёжную цепочку планирования, учёта и распределения затрат по всему циклу воспроизводства научно-технического продукта в настоящее

время очень и очень трудно. Это подтверждает тот вывод, что выстраивание таких цепочек − не узко производственная, а социально-экономическая и экономико-политическая задача. Необходимо восстановить связи фундаментальной академической и вузовской науки, которая всегда была сильна своими флагманами, такими как, например, Физтех, МИФИ, МГТУ им. Н.Э. Баумана, МАИ, Санкт-Петербургский государственный морской технический университет, с крупными холдингами, их прикладными структурами, конструкторскими и технологическими бюро. Для начала следует теоретически сформулировать данную задачу, затем наладить такое взаимодействие научных и корпоративных структур, чтобы государственно-частное партнёрство приносило взаимную выгоду. Дополнительная сложность – организация взаимодействия в условиях рыночной экономики, требующая иных по сравнению с существовавшими в советское время механизмов продвижения научной идеи вплоть до получения конечного продукта. Для решения поставленной задачи государство должно проводить связную научно-техническую политику, научиться понимать, что такое наука, каковы апробированные в мировой практике механизмы её финансирования и формирования новых институций, и перестать заниматься пустой имитацией зарубежного опыта. Неудачные реформы могут нанести серьёзный удар по консолидации научных исследований в интересах ОПК. Это справедливо и в отношении реформы РАН, одним из основных шагов которой является создание особого федерального агентства по управлению имуществом академии. Отвлекаясь от закулисных мотивов такого решения, отметим: данная модель отчасти повторяет определённые черты китайских академических реформ с той лишь разницей, что там государство реализует специфическую модель соединения фундаментальных исследований и инноваций с рыночными, в том числе корпоративными формами организации науки высокого уровня. Существенно, что в Китае используется дифференцированный подход к интеллектуальной собственности и активам в зависимости от источника их происхождения. То, что принадлежит государству, контролируется им с позиций защиты интересов страны. Но государство защищает и права, и интересы научных структур и их трудовых коллективов там, где это касается интеллектуальной собственности и активов, созданных и принадлежащих институтам или их научно-инновационным фирмам. При этом оно не прибегает к специальным административным методам и одновременно ведёт беспощадную войну с коррупцией в органах государственной власти. В России создание новых государственных структур часто преследует цели нейтрализации негативных последствий ранее принятых политических или управленческих решений, искусственно созданного дефицита управления, устранения кризисных ситуаций. Расширение поля государственного контроля без достаточ-

ных объективных потребностей и оснований редко даёт ожидаемый эффект и сопровождается разрастанием госаппарата, усилением бюрократизма в управлении, а как следствие, ростом и без того высокого уровня коррупции.

Заимствование американской модели при явном ослаблении академии потребует адекватного усиления не только университетской науки, которая в США сильна лишь в области открытых исследований, где для оценки эффективности науки преимущественно используются показатели цитируемости.

Большинство прорывных исследований осуществляется в национальных и корпоративных лабораториях и исследовательских центрах в интересах национальной безопасности по заказам соответствующих структур (Минобороны, спецслужб, НАСА). У нас тоже есть проекты типа «1000 лабораторий», «1000 национальных исследовательских центров». Но за редким исключением они не сопоставимы ни с отдельными американскими организациями, ни тем более с их научной инфраструктурой в целом. Даже небольшое сокращение 3–10-кратных разрывов в уровне зарплат, достижение приборной и технологической обеспеченности, финансово-экономической мощи, сравнимых с показателями американских научных институтов и университетов, потребует триллионных затрат в рублёвом исчислении. Характерная для российских реформ неуправляемость имеет свою цену в виде потерь от инвестиционно-инновационного и структурного застоя и последующего снижения экономического роста.

Для того чтобы ответить на возникающие вызовы, нашей стране необходимо сохранять науку и образование и существенно глубже интегрироваться в мировую инновационную систему, преодолевая сохраняющуюся изоляцию. В противном случае «окна возможностей» для перехода к инновационной экономике будут сужаться, пока ещё сохраняющийся научный потенциал таять, геополитические позиции ослабевать, а уровень военной безопасности неминуемо снижаться. В результате России грозит превращение в страну с инновационной системой имитационного типа, не способной к производству нового знания и достижению глобального лидерства по ключевым технологическим направлениям, для которой характерно долговременное закрепление сырьевого типа экономики и низкие темпы экономического роста. Стране нужна не только реиндустриализация, предполагающая восстановление утерянного и повторение пройденного, но и «ремодернизация». Советское общество было обществом с высокоразвитым социально-культурным и социально-экономическим потенциалом. Образование, воспитание, наука, культура обеспечивали интенсивное воспроизводство интеллектуального капитала общества. Идеалом был образ человека-творца, мотивированного на уважение к традиции, нравственности, культуре, знанию, почти религиозную веру в будущее. Эти

качества, считавшиеся в советском обществе высшими ценностями, сегодня в значительной мере утрачены. Нужно вернуться к ценностям той модернизации, которую Россия выстрадала в ходе своей великой и трагической истории, возрождая и умножая своё духовное, культурное, научное и экономическое наследие. Это и есть необходимое условие прогресса и экономики, и фундаментальной науки, и системы военной безопасности, и оборонно-промышленного комплекса [70].

Технологические угрозы представляют серьезную опасность для российской экономики и, в связи с этим, государство должно принять адекватные меры по их нейтрализации.

В долгосрочной перспективе необходимо сосредоточится на поисках альтернативных путей развития микроэлектроники и компьютерной техники, основанных на принципиально новых принципах обработки информации. За рубежом проводятся активные исследования и разработки в области создания молекулярных (био-) компьютеров и процессоров с использованием оптических, органических, квантовых устройств [71]. Для оперативного решения текущих задач следует исключить применение в проектировании материалов и комплектующих зарубежных поставщиков, чувствительных к влиянию политической конъюнктуры. При проектировании ракетно-космической и оборонной техники следует использовать отечественную электронно-компонентную базу (ЭКБ), что, возможно, и приведет к снижению некоторых эксплуатационных характеристик части изделий, но сохранит приемлемый уровень экономической безопасности стратегически важных отраслей промышленности.

Программа импортозамещения должна носить комплексный характер и способствовать не только снижению зависимости от зарубежных партнеров, повышению уровня экономической безопасности, но и стимулировать рост и конкурентосопосбность отечественной промышленности.

Государство также не в состоянии профинансировать замену всего спектра материалов и комплектующих, получаемых по импорту. Для обеспечения достаточного уровня независимости от импорта, необходимо в приоритетном порядке профинансировать модернизацию стратегического сектора промышленности, среди которых наиболее важное значение имеет производство электронной компонентной базы (ЭКБ). Отставание в этой сфере в настоящий момент носит критический характер для развития практически всех высокотехнологичных производств. Разумеется, нет нужды отказываться от импорта всей ЭКБ, включая резисторы, конденсаторы и прочие элементы, их следует импортировать из различных независимых друг от друга стран и производителей. Что касается радиационно устойчивых ЭКБ, сетевых контроллеров, микропроцессоров с высокой плотностью элемен-

тов, то здесь необходимо срочно осваивать новые технологии, закупать оборудование последнего поколения для их производства, финансировать исследования и разработки. Для снижения стоимости выпускаемой для отечественных потребителей техники, следует максимально расширить область ее применения. Продукция должна широко использоваться не только в военной и аэрокосмической промышленности, но и в гражданском секторе экономики. Радиационно стойкие и миниатюрные электронные приборы используются в промышленности в рентгеновской дефектоскопии, медицинской технике, в ядерной энергетике, научной аппаратуре и др. Это позволяет повысить массовость выпуска и получить экономию за счет эффекта масштаба, что дает возможность снизить цену на выпускаемую продукцию и захватить достаточно большой сегмент рынка.

Программа импортозамещения в сфере информационных технологий может быть успешно реализована, если будет не только освоен выпуск современной компьютерной техники, но и создан спрос на нее у отечественных и зарубежных потребителей. Компьютерная техника, попадающая под программу импортозамещения, должна работать исключительно с отечественными программами автоматизации управления и базами данных.

Решение проблемы импортозависимости классическая экономическая теория видит в стимулировании спроса предприятий потребителей оборудования и в стимулировании предложения отечественных производителей. Увеличить выпуск наукоемкой продукции на отечественных предприятиях можно только после их значительной модернизации, что потребует колоссальных затрат материальных ресурсов и времени. Кроме того, потребуется проведение существенного объема работ по технической подготовке производства, включающих в себя научно-исследовательские, опытно-конструкторские и технологические работы, за время проведения которых, возможно моральное устаревание проектируемой техники. Значительные затраты и длительность процесса снижают инвестиционную привлекательность проекта модернизации, что делает маловероятным его реализацию. В этой схеме отечественные предприятия ставятся на позицию имитатора, догоняющего индустриально развитые экономики мира.

Стимулирование спроса на отечественное ПО, оборудование и электронные приборы может быть реализовано, по мнению ряда экономистов, посредством предоставления преференций покупателям отечественной продукции, к числу которых можно отнести налоговые льготы, участие в реализации госзаказа [72], компенсация ставок по кредитам [73], хотя льготное кредитование предприятий не всегда приносит ожидаемый эффект, так как выделяемые на развитие технологиче-

ской базы ресурсы, направляются, по мнению председателя ЦБ РФ Эльвиры Набиуллиной, на имущественные сделки по слиянию и поглощению [74].

Авторы полагают, что наиболее эффективным методом стимулирования спроса является финансовый и оперативный лизинг отечественного оборудования с государственной поддержкой. В соответствии с лизинговыми схемами, предприятие получает для производственных нужд технологическое оборудование в долгосрочное пользование с пониженным арендным тарифом, включающим в себя ремонт и регламентное обслуживание техники на весь срок действия договора. Предприятия, участвующие в реализации гособоронзаказа и федеральных целевых программ, могут получать от государства отечественное оборудование в счет будущих расчетов за поставленную по контрактам продукцию.

Нивелированию технологических угроз будет способствовать диверсификация зарубежных поставщиков материалов, комплектующих и оборудования. По мнению авторов, не имеет смысла полностью отказываться от импорта высококлассного оборудования, материалов и инструментов, однако при заключении внешнеторговых и инвестиционных сделок, следует убедиться в независимости поставщиков от возможного внешнего политического давления.

В целом, не смотря на относительную высокую импортозависимость в российской промышленности, в ближайшие пять лет можно переломить негативный тренд и выйти на приемлемые уровни закупок отечественного оборудования, что снизит восприимчивость экономики России к технологическим угрозам.

2.5. Система информационной безопасности

Процессы информатизации охватили практически все страны, вышедшие на постиндустриальный этап развития, который характеризуется возрастающей ролью информации в жизни общества. На этом этапе главным ресурсом все чаще вместо вещества, энергии, капитала становится информация. Успех производственной и предпринимательской деятельности, экономическая мощь развитых государств в значительной мере стали зависеть от умения эффективно распоряжаться таким ценнейшим стратегическим ресурсом, в какой превратилась информация [75, 76]. Как известно, ресурсами считаются элементы экономического потенциала, которыми располагает общество и которые используются для достижения конкретных целей хозяйственного и социального развития. Назначение традиционных видов ресурсов (материальные, финансовые, трудовые, природные и другие) и способы их применения вполне понятны. Под информационными ресурсами понимаются документы и их массивы в различных формах и видах, содержащие

сведения по всем направлениям общественной деятельности. Поэтому собственность современного предприятия – это не только машины, оборудование, сырье и т.д., но и идеи, концепции, знания, технологии (интеллектуальный потенциал), т.е. все то, что превращается в товары и услуги, направляемые на удовлетворение материальных и духовных потребностей населения. Важнейшей характеристикой информации считается ее ценность (полезность), которая, как правило, определяется ее владельцем. Несмотря на многочисленные попытки формализовать этот процесс с помощью различных методов теории информации и исследований операций, процедура оценки пока остается достаточно субъективной. В зависимости от этой характеристики собственник решает, нужно ли держать информацию втайне от конкурентов и как защищать ее от всевозможных посягательств. При этом важным критерием при выборе защитных средств выступает прибыль (реальная или потенциальная), приносимая используемой информацией. Для владельца ценность должна соизмеряться со стоимостью процесса защиты информации, а для конкурентов – компенсировать затраты на ее получение. Другой значимой характеристикой информации представляется ее важность. По уровню важности можно предложить следующее распределение информации по категориям [77]:

- принципиально важная (незаменимая), наличие которой необходимо для функционирования предприятия;
- важная, которая может быть заменена или восстановлена, но эти процессы трудоемки и связаны с большими затратами;
- полезная, которую трудно восстановить, но предприятие может эффективно функционировать и без нее;
- несущественная, которая больше не нужна предприятию.

На практике процедура отнесения информации к одной из перечисленных категорий представляется достаточно сложной задачей, поскольку одна и та же информация может использоваться многими подразделениями предприятия, каждое из которых по-разному определяет категорию важности этой информации. Категория важности, как и ценность, изменяется со временем и зависит от отношения к ней различных категорий потребителей. На основании анализа ценности и важности определяются информационные массивы, которые составляют секреты предприятия – производственную и коммерческую тайну. Сведения из этих массивов сознательно скрываются от посторонних, поскольку они определяют истинное социально-экономическое и научно-техническое состояние предприятия.

Информационные сведения, требующие защиты. Для выявления сведений, требующих защиты, необходимо четко представлять виды информации, составляющие государственную, производственную и коммерческую тайну. В связи с тем,

что вопросу зашиты государственной тайны достаточно подробно и системно рассмотрены, в рамках данной статьи внимание целесообразно сконцентрировать на информации, закрытой в интересах отдельных хозяйствующих субъектов. Согласно существующему законодательству к производственной тайне относятся сведения технического, экономического и организационного характера, которые зависят от способа производства, технологии, организации труда, а также технологические открытия, изобретения, информация о целях и характере исследовательских работ. Коммерческой тайной являются сведения, относящиеся к торгово-финансовой сфере деятельности предприятия. Эти сведения можно сгруппировать по тематическому принципу и с учетом отличительных особенностей каждого конкретного предприятия условно представить в виде следующего перечня:

- финансовые документы (прибыль, фонд заработной платы, финансовые отчеты и прогнозы, банковские счета и т.п.);
- информация о рынках сбыта (история, объем, тенденции производства, стратегия цен и маркетинг, планы и рыночная политика, реклама, политика и методы сбыта т.п.);
- данные о производстве и продукции (производственные мощности, номенклатура изделий, технические спецификации перспективной и существующей продукции, технический уровень и сроки создания разрабатываемых изделий и т.п.);
- сведения о поставщиках и потребителях.

Рыночные отношения способствуют усилению конкуренции не только в сфере международной торговли, но и между отдельными предприятиями, производящими однотипную продукцию. Поэтому несанкционированный доступ и использование информации, не предназначенной для распространения, уже сейчас наносит многим предприятиям значительный ущерб. Проводимые за рубежом и российскими научно-производственными коллективами исследования убедительно показывают, что для предприятий различной формы собственности весьма актуальной и значимой становится проблема защиты информации, представляющей интерес для конкурентов или иных лиц, которые способны использовать ее в своих целях.

В условиях административно-планового народного хозяйства на предприятиях существовала хорошо организованная и эффективно действующая система охраны государственных секретов. Однако вместе с тоталитаризмом она была разрушена. Становление и развитие новых форм собственности, обвальная приватизация, направленная на разгосударствление экономики, ряд других обстоятельств привели к смене владельцев многих предприятий. К руководству пришли люди, слабо представляющие особенности рыночного производства и, в том числе, не

сразу осознавшие необходимость охраны общественных и собственных секретов. Практика функционирования экономики в переходных условиях заставила обратить самое серьезное внимание на проблемы национальной безопасности [78], в частности, на обеспечение безопасности в информационной сфере [79].

Прежде, чем перейти к рассмотрению собственно проблем информационной безопасности, напомним, что традиционно информационная система (ИС) определяется как организационно упорядоченная совокупность технических средств, информационных ресурсов и технологий, реализующих информационные процессы в ручном или автоматизированном режимах в целях полного, точного и оперативного удовлетворения информационных потребностей пользователей.

С появлением сложных автоматизированных информационных систем проблема обеспечения защиты информации от несанкционированного доступа становится все более актуальной по ряду причин, основными среди которых можно считать следующие [80]: значительный рост объемов сведений, накапливаемых, обрабатываемых и распространяемых с помощью средств и устройств вычислительной техники; интеграция в единых базах и банках данных сведений различного назначения; расширение категорий пользователей, имеющих доступ к информационным ресурсам автоматизированных систем; усложнение режимов работы технических средств, образующих сложные вычислительные системы (внедрение многопрограммных и многопроцессорных режимов, разделения времени и т.п.); увеличение количества внешних устройств и программно-технических связей в автоматизированных информационных системах.

Обеспечение безопасности ИС – это меры, предохраняющие систему от преднамеренного или случайного вмешательства в режимы ее работы. Следует подчеркнуть, что в политике информационной безопасности нет мелочей, так как ни одна система не является абсолютно безопасной. Не существует единого универсального решения, обеспечивающего абсолютную защиту ИС, поэтому следует адаптировать существующие методы и средства в зависимости от реальных и потенциальных угроз, размеров возможного ущерба и расходов на обеспечение приемлемой безопасности. Необходимо отметить, что к числу особо сложных компонентов ИС любой природы относятся люди (сотрудники, продавцы, партнеры, клиенты и т.д.), являющиеся главными источниками информации. Поэтому работа с кадрами – важнейшее направление деятельности по обеспечению сохранности конфиденциальной информации и защиты ее от несанкционированного доступа.

Необходимо изучать весь состав работающих на предприятии специалистов, выделяя при этом тех, кто имеет доступ к особо ценной и важной информации. Особые категории работников – это кандидаты на вакантные должности и на

увольнение. Эти люди, в большей мере, чем остальные, склонны к противоправным действиям, особенно последние. Объектом повышенной заботы должен быть персонал, осуществляющий сбыт продукции и обслуживающий запросы клиентов о возможностях улучшенных или новых моделей, планируемых к реализации. Сообщая дополнительную информацию о разрабатываемых изделиях, такие специалисты могут разгласить сведения, составляющие производственную или коммерческую тайну.

Основные положения безопасности ИС. В настоящее время сложились вполне конкретные концепции и инфраструктура защиты информации, базовыми элементами которой являются: развитый арсенал технических и аппаратных средств защиты, создаваемых на промышленной основе; большое количество фирм, специализирующихся на решении проблем защиты информации; четко определенная концептуальная система взглядов на информационную безопасность. Обширный практический опыт свидетельствует о том, что: процесс обеспечения надежной безопасности ИС должен быть многоразовым актом, постоянно и непрерывно совершенствующийся во времени; информационная безопасность обеспечивается только при комплексном и системном использовании всех имеющихся средств и методов защиты во всех производственных структурных элементах и на каждом технологическом этапе процедуры обработки информации и изготовления продукции; функционирование механизмов защиты должно постоянно контролироваться, дополняться и обновляться в зависимости от изменения внутренних и внешних условий, с учетом возможных угроз различного происхождения; без профессионального обучения пользователей и без надлежащего соблюдения ими всех установленных правил и требований сохранения конфиденциальности невозможно обеспечить требуемый уровень безопасности.

В соответствии с принципами системного подхода процесс информационной защиты должен быть: постоянным (злоумышленники постоянно ищут малейшую возможность для того, что обойти защиту); плановым (планирование выполняется разработкой каждым подразделением подробных планов защиты, учитывающих главную цель предприятия в целом); централизованным (организационно-функциональная самостоятельность процедуры обеспечения безопасности должна осуществляться в рамках определенной структуры); конкретным (защищать следует конкретные данные, потеря которых может причинить организации серьезный ущерб); активным (информационная защита должна осуществляться целеустремленно и настойчиво); надежным (перекрываться должны все возможные каналы и способы утечки); целенаправленным (защищается не все подряд, а только информация, используемая в рамках некоторой конкретной цели); универсальным (необ-

ходимо ограничиваться разумными и достаточными средствами, по возможности расширяя их возможности для решения возникающих задач); комплексным (необходимо в полном объеме применять все виды, формы и методы обеспечения безопасности).

Система информационной безопасности (СИБ) способна снижать инвестиционные и инновационные риски предприятия [81] и должна удовлетворять следующим основным условиям, в частности: охватывать весь технический и технологический процесс информационной деятельности каждого предприятия; позволять проведение дополнений и изменений мер обеспечения информационной безопасности; быть разнообразной по применяемым средствам и методам, многоуровневой с различной последовательностью доступа к информации: быть нестандартной, оригинальной в реализации возможностей защиты; быть удобной для технического обслуживания и простой для эксплуатации непрофессиональными пользователями. К СИБ предъявляются следующие дополнительные требования: четкое определение полномочий и прав пользователей к доступу на работу с определенными видами информации; предоставление каждому пользователю минимальных инструментальных полномочий, позволяющих ему выполнить порученные работы; сведение к минимуму количества общих для разных пользователей средств и методов защиты; учет все попыток и случаев несанкционированного доступа к защищенной конфиденциальной информации; обеспечение контроля за состоянием средств защиты информации и немедленное реагирование в случае выхода их из строя; обеспечение качественной и количественной оценки уровня конфиденциальности информации. СИБ обязана иметь надежные механизмы собственного обеспечения, на основе которых она сможет успешно и эффективно выполнить свое предназначение, в частности, в системе должны быть предусмотрены:

- правовое обеспечение (правовые документы, нормативные акты, инструкции, руководства и т.п., требования, выполнение которых обязательно в рамках области их действия);
- организационное обеспечение (осуществление информационной безопасности выполняется определенными структурными подразделениями, такими, как, например, служба безопасности предприятия);
- информационное обеспечение (сведения, показатели, данные, параметры, используемые при решении основных задач, обеспечивающих успешное функционирование СИБ);
- техническое обеспечение (аппаратные средства, предназначенные не только для защиты информации, но и для осуществления эффективной деятельности СИБ);

- математическое обеспечение (методы, используемые для расчетов, позволяющих оценить опасность используемых злоумышленниками разведывательных технических средств, норм и зон необходимой защиты);
- программное обеспечение (информационные, учетные, математические, статистические, когнитивные и расчетные программы, обеспечивающие оценку опасности и наличия методов несанкционированного доступа к информации и различных каналов ее утечки);
- лингвистическое обеспечение (комплекс специальных языковых инструментов общения пользователей и специалистов в сфере обеспечения информационной безопасности);
- нормативно-методическое и регламентное обеспечение (нормы и регламенты, формализующие деятельности органов, средств, служб, реализующих основные функции защиты информации, методики, обеспечивающие надлежащими правилами деятельность пользователей при работе с закрытой и конфиденциальной информацией).

Основной целью СИБ является предотвращение ущерба ИС и интересам отдельного предприятия, наносимому за счет хищения материально-технических и финансовых средств, нарушения процесса функционирования технических средств ИС, уничтожения ценностей и имущества, разглашения, утраты, уничтожения, утечки, искажения информации, а также физическая защита персонала [82]. Для этого СИБ должна обеспечить: защиту прав предприятия, всех его подразделений и работающих на нем сотрудников, эффективное использование и сохранность материальных, информационных и финансовых ресурсов; повышение престижа и рост прибылей за счет обеспечения высокого качества услуг по безопасности поставщиков, партнеров и клиентов.

Основными задачами, решаемыми СИБ являются:

- выявление и нейтрализация угроз безопасности, условий, причин и прочих обстоятельств, способствующих нанесению серьезного ущерба интересам предприятия, нарушению его прогрессивного инновационного развития и нормального функционирования;
- отнесение информации к различным категориям ограниченного использования и доступа, к различным уровням опасности (уязвимости) и подлежащих соответствующей ситуации защите;
- создание условий и методов оперативного реагирование на появляющиеся угрозы безопасности, приводящие к негативным явлениям в функционировании предприятия;

- эффективное и быстрое пресечение посягательств на ресурсы предприятия и угроз персоналу;
- разработка и реализация механизмов, обеспечивающих быструю локализацию опасных зон вмешательства в деятельность предприятия и максимального возмещения наносимого ущерба, ослабление негативных последствий на процесс достижения целей предприятия, возникающих вследствие нарушения безопасности.

Объектами, подлежащими защите от потенциальных внутренних и внешних угроз и противоправных действий, являются: персонал, материальные, финансовые, интеллектуальные и информационные ресурсы, средства и системы информатизации и охраны всех видов ресурсов. Основными задачами обеспечения безопасности и надежной защиты информационных ресурсов являются: осуществление закрытой переписки и шифровальной связи; построение и практическая реализация системы, разрешающей работу исполнителей со сведениями и документами ограниченного доступа; планирование и координация работ по обеспечению защиты информации, накапливаемой, систематизируемой, обрабатываемой и распространяемой средствами ИС; обеспечение безопасности в ходе проведения конфиденциальных переговоров, совещаний и деловых встреч; осуществление действенного контроля за сохранностью закрытых и конфиденциальных документов, за обеспечением эффективной защиты информации, собираемой и обрабатываемой средствами ИС; организация учета, хранения и использования конфиденциальных документов и их носителей.

Основными принципами обеспечения информационной безопасности являются взаимная ответственность руководства и персонала предприятия, законность, достаточность, взаимодействие с государственными и частными правоохранительными органами, соблюдение оптимального баланса интересов предприятия и личности.

Основными направлениями обеспечения безопасности информации выступают инженерно-техническое, организационное и правовое обеспечение.

Правовое обеспечение безопасности ИС. В настоящее время вопрос о правовом обеспечении процессов информатизации активно прорабатывается как в законотворческом, так и в практическом плане. В качестве предметов правового регулирования должны рассматриваться: правовой режим информации, средств и индустрии информатизации и систем информационных услуг, средства и формы защиты информации; правовой статус каждого участника правоотношений в процессах производственной и социально-экономической информатизации (определение права на информацию, гарантий и защиты прав и установления ответственности в зависимости от ролей субъектов); порядок взаимоотношений всех субъектов,

участвующих в информатизации, с учетом их изменяющегося правового статуса на всех уровнях и на различных стадиях процесса функционирования ИС.

Особое значение приобретают проблемы: экономики информатизации – выработка правовых методов и механизмов информационного обеспечения предприятия, распределения, анализа, обмена, потребления и надежной защиты информационных ресурсов; информационной безопасности – надлежащая защита общества и личности от отрицательных последствий процессов информатизации, обеспечение правопорядка отношений в области информатизации; информационной метрологии, стандартизации, нормативное закрепление понятийного и терминологического аппарата в области информатизации.

Законодательство, определяющее и регламентирующее информационную безопасность, является неотъемлемой частью российских законов, в том числе: конституциональное законодательство; общие основополагающие законы (о собственности, о налогах, правах и т.д.); законы, связанные с организацией управления отдельными хозяйствующими структурами, с экономикой, с финансами, с государственными органам и системой, определяющей их статус; правоохранительное законодательство; специальные законы, относящиеся к конкретным областям отношений, процессам, отраслям хозяйства и производственным комплексам; подзаконные и другие нормативные акты, связанные с процессами информатизации.

К правовому обеспечению следует отнести такие документы как составление трудовых договоров на проведение производственных и других работ, в том числе и по оказанию различных информационных услуг. При этом правовая гарантия определяется предусмотренными условиями ответственности в случае нарушения сторонами взятых на себя обязательств. Стороны могут также прибегнуть к страхованию убытков. В договоре определяют, какая сторона должна заключить соответствующий договор со страховой кампанией. Обычно, страхование осуществляет исполнитель, но в этом случае страховая сумма включается в цену выполняемых работ. Организационное обеспечение безопасности ИС. Совокупность действий или процессов, ведущих к возникновению и совершенствованию взаимоотношений (взаимосвязей) между отдельными частями единого целого, принято считать организационными мероприятиями. К организационным мероприятиям следует отнести: специальные действия, выполняемые при проектировании, строительстве и обустройстве производственных зданий и помещений; подбор персонала, обучение его основам, правилам и методам работы с конфиденциальной информацией, ознакомление с ответственностью, предусмотренной за нарушение правили требований защиты информации и т.д.; организация, поддержание и совершенствование надежного контроля за действиями посетителей и пропускного

режима; организация надежной охраны территорий и помещений; организация использования носителей и документов конфиденциальной информации и их хранения, включая порядок учета, выдачи, исполнения и возвращения; назначение ответственного за защиту информации, проведение систематического контроля за персоналом, работающим с конфиденциальной информаций и т.д.

Одним из основных направлений организационных мероприятий является четкая организация системы делопроизводства и документооборота. Основным организационным мероприятием является разработка перечня охраняемых сведений и проведения аттестации помещений на предмет выработки конкретных мер по защите и обеспечению безопасности конфиденциальной информации. Важным мероприятием представляется создание на предприятии собственной службы безопасности – системы штатных органов управления и организационных формирований, предназначенных для обеспечения безопасности и защиты конфиденциальной информации. Эффективность обеспечения экономической [83] и, в частности, информационной безопасности предприятия может быть наивысшей, если работа в службе безопасности будет престижной и высоко оплачиваемой. Интересна практика защиты информации в США.

Кратко рассмотрим методологию системного подхода к организации и функционированию системы защиты конфиденциальной информации, названной методом Operation Security («Opsec»). Метод универсальный и может быть использован как для защиты технологической и коммерческой тайны, так и для обеспечения сохранности государственных секретов. Суть метода состоит в том, чтобы предотвратить, пресечь или ограничить доступ к той части информации, которая позволит конкуренту «вычислить» или узнать, какой новый инновационный товар планирует произвести предприятие, чтобы опередить его на рынке, создав аналогичную продукцию раньше и дешевле.

Процесс защиты информации по данному методу проходит поэтапно:

- начальный этап (анализ и изучение объекта защиты) заключается в определении, что следует защищать (какие виды информации требуют защиты, наиболее значимые элементы защищаемой информации, определяется жизненный цикл критической информации и т.д.);
- на втором этапе осуществляется выявление потенциальных угроз (выявляется, кого может заинтересовать защищаемая информация, изучаются методы, которые используют конкуренты для ее получения, оцениваются возможные каналы утечки информации, разрабатывается система мероприятий по пресечению действий конкурентов);

- на третьем этапе определяется эффективность подготовленных и постоянно действующих подсистем обеспечения безопасности;
- на четвертом этапе принимаются дополнительные необходимые средства и меры по обеспечению информационной безопасности;
- на пятом этапе руководителями организации изучают и оценивают представленные рекомендации для осуществления предложенных мер безопасности, выполняют расчет их стоимости и эффективности;
- на шестом этапе осуществляется реализация одобренных мер безопасности в соответствии с установленными приоритетами; заключительный этап предусмотрен для проведения контроля и доведения до персонала предприятия мер безопасности, принятых к реализации.

Для практического внедрения данного метода необходимо участие команды аналитиков, являющихся высококвалифицированными специалистами не только в области информатики, но и в тех научных областях, знания из которых используются при выполнении аналитических исследований. Организация аналитической работы включает три основных направления: о рынке, о производстве и продукции, об организационных особенностях и финансах.

Инженерно-техническое и технологическое обеспечение безопасности ИС предприятия. Инженерно-техническая и технологическая защита – это совокупность технических средств и специальных органов, а также организационных мероприятий по их комплексному использованию в интересах обеспечения безопасности предприятия. По функциональному назначению инженерно-техническая и технологическая защита использует следующие средства:

- физические, которые включают различные инженерные сооружения и средства, препятствующие проникновению злоумышленников на защищаемые объекты и осуществляющие защиту информации, материальных средств, персонала, и финансов от противоправных действий; аппаратные, в число которых входят приборы, приспособления, устройства, а также разнообразные технические решения, начиная от телефонного аппарата и кончая самыми современными автоматизированными ИС;
- программные, представляющие собой специальные программные комплексы, отдельные программы и системы разноплановой защиты информации; криптографические – специальные алгоритмические и математические средства, основанные на применении методов шифрования.

Шифрование является механизмом эффективной логической безопасности. Оно может использоваться в интересах обеспечения и целостности, и конфиденци-

альности как хранимой, так и передаваемой информации. Самой определяющей частью системы шифрования является генерация и передача ключей. Физическая безопасность не сводится к безопасности только вычислительного центра, тем более что ИС все более и более рассредоточиваются. Необходимо рассматривать взаимосвязь безопасности комплекса знаний, сооружений и оборудования. Безопасность ИС оценивается на основе использования таких мер, как идентификация, подтверждение подлинности, контроль доступа, информационные права, аудит, безаварийность и конфиденциальность. Особо следует рассмотреть систему разграничения доступа к конфиденциальной информации. Защита ИС в линиях связи сводится к защите содержания сообщения и защите процесса передачи данных.

Искусственный интеллект в системе безопасности экономической системы. Широкое использование информационных технологий во всех видах экономической деятельности создало целую серию ранее неизвестных угроз, в число которых входит не только хищение денежных средств со счетов юридических и физических лиц, но и потеря управления предприятием и его внешними связями с поставщиками материалов, сырья и потребителями продукции, сбои в системах автоматизированного управления технологическими процессами и др. Эти и другие проблемы могут быть вызваны как намеренными действиями злоумышленников, так и случайными факторами. Классическим примером атаки на производственные структуры компаний является диверсия на иранских предприятиях, занятых обогащением урана, совершенная Израилем в 2009 г. В систему управления была внедрена вирусная программа Stuxnet, которая представляет собой компьютерный червь, перехватывающий и модифицирующий информационный поток между компьютерами, управляющими технологическими процессами. Для решения проблем, связанных с экономической безопасностью предприятия, на базе технологий искусственного интеллекта (ИИ) были созданы компьютерные программы и устройства, которые сейчас достаточно широко используются, прежде всего, в финансовой сфере. Специальные программы помогают распознавать и блокировать подозрительные трансакции, другие, по ряду признаков, позволяют идентифицировать личности клиентов и соискателей. Эти программы дополнены бесконтактными детекторами лжи, которые позволяют объективно оценить качества потенциального работника.

В настоящий момент практически во всех финансовых организациях созданы специальные службы информационной безопасности, которые получили название «Комплаенс». Этот термин означает, в переводе с английского языка compliance – соответствие, что означает способность организации соответствовать

законодательству, стандартам, нормам и правилам, сформировавшимся в бизнес-среде [84].

Центральный Банк России уже принял соответствующее положение, согласно которому во всех банках, страховых организациях и финансовых компаниях вводится служба комплаенс-контроля, которая ориентирована на так называемые регуляторные или комплаенс риски [85]. Центральный банк Положением № 242-П определяет комплаенс-риск, как риск «возникновения у кредитной организации убытков из-за несоблюдения законодательства Российской Федерации, внутренних документов кредитной организации, стандартов саморегулируемых организаций, а также в результате применения санкций и (или) иных мер воздействия со стороны надзорных органов» [85].

В более широком понимании, комплаенс-риски представляют собой вероятность финансовых, материальных, репутационных и иных потерь вследствие нарушения как внешних, так и внутренних норм и правил ведения экономической деятельности. Если проблема организации комплаенс контроля в финансовых учреждениях достаточно хорошо исследована [86–88], то вопросы использования метода в индустрии остаются, в силу специфики промышленного производства, еще открытыми.

Для сохранения уровня конкурентоспособности отечественной экономики, необходимо вводить системы ИИ типа «Комплаенс», не только в банках, но и на промышленных предприятиях, строительных компаниях и органах государственного и местного управления. Комплаенс риски могут оказывать влияние на организацию не только в финансах, но и других, не менее важных сферах деятельности, к которым относится производство, снабжение и сбыт, трудовые отношения и др.

Комплаенс риски предлагается условно разделить на внутренние и внешние. К внутренним рискам отнесем те, которые имеют отношение к взаимодействию подразделений предприятия, материальным потокам между производственными и вспомогательными цехами, участками, складами. Механизм управления производственными комплаенс рисками представлен на рис. 3.

Механизм управления производственными комплаенс-рисками (рис. 3) функционирует следующим образом. Производственные подразделения предприятия укомплектованы технологическими линиями с датчиками, передающими информацию о протекании техпроцессов (время обработки деталей на операциях, время перерывов, количество изготовленных изделий, расход материалов, энергии и др.) Поступающая информация анализируется на предмет соответствия фактического протекания техпроцесса технологии, прошитой в базе технологических процессов. Параллельно проводится анализ запасов материалов, комплектующих,

обеспечивающих нормальное протекание техпроцесса, на предмет количества и соответствия требованиям технологической документации. Любое нарушение стандартов в производственной системе может привести к сбою технологического процесса, остановке производства, срыву плана поставок и другими проблемами. Здесь важную роль играет процесс обеспечения цехов и участков предприятия материалами, сырьем, комплектующими, услугами, который должен соответствовать стандартам производства. Искусственный интеллект формирует для менеджмента предприятия несколько вариантов возможного решения проблемы и оперативно устраняет несущественные сбои и отклонения от стандартов. Например, при выявлении дефицита на складах предприятия необходимого количества комплектующих, ИИ информирует соответствующие службы и формирует заказ на поставку нужных для производства компонентов. ИИ может выявлять не только проблемы, связанные с технологическим процессом, но и пресекать попытки использования имеющихся на предприятии ресурсов не по назначению. Вместе с тем, как отмечают зарубежные исследователи, искусственный интеллект может сам стать источником рисков. Несанкционированное проникновение в программу может нанести существенный ущерб предприятию.

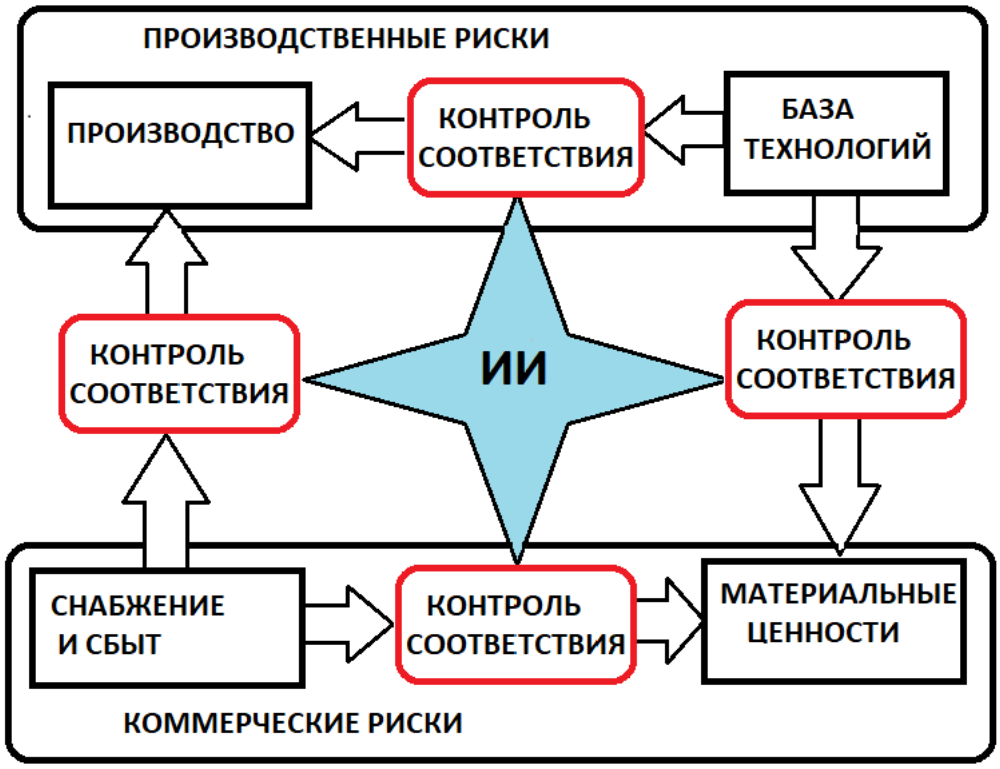

Рис. 3. Модель механизма управления внутренними производственными комплаенс-рисками [89]

К внешним рискам отнесем риски неисполнения контрактных обязательств, финансовые и репутационные риски. Модель механизма управления внешними комплаенс рисками представлена на рис. 4.

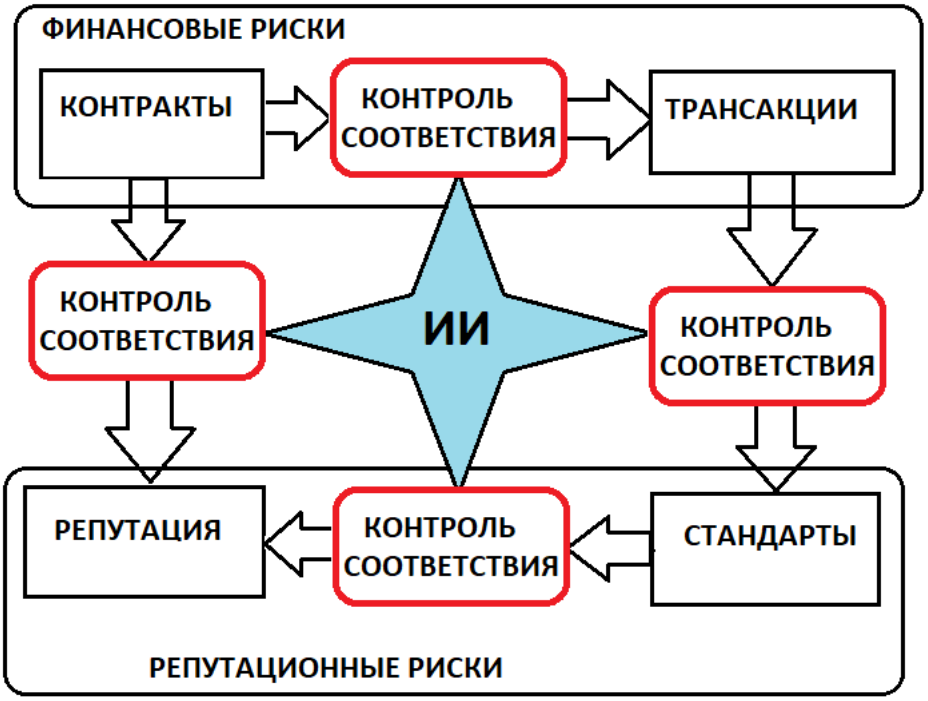

Рис. 4. Механизм управления внешними комплаенс-рисками [89]

Финансовые риски могут реализоваться в случае осуществления трансакций в пользу сомнительных контрагентов, оплаты необусловленных контрактами счетов, задержки платежей по расчетам с партнерами, которые чреваты начислением пенни, неустоек, штрафов и судебными издержками. Несоблюдение организацией контрактных обязательств, как показано на рис. 4, ведет к репутационным потерям, которые могут существенно повлиять на функционирование предприятия. Сомнительная бизнес-репутация предприятия не способствует заключению новых контрактов на выгодных условиях, снижению банковской ставки по кредитам, найму высококвалифицированной рабочей силы. ИИ может выделять сомнительные трансакции и вовремя их блокировать. Кроме того, ИИ в состоянии анализировать бизнес-информацию, распространяемую в СМИ, касающуюся организации и оповещать руководство и собственников компании о различных негативных публикациях, агрессивной рекламе конкурентов и проч. ИИ осуществляет непрерывный мониторинг законодательной базы, международных соглашений, введении новых норм и правил, которые касаются деятельности предприятия и сравнивают с действующими на предприятии положениями и стандартами. В случае выявления отклонений, система оповещает руководство организации и формирует варианты

решения возникшей проблемы. ИИ можно доверить и автоматическое внесение непринципиальных изменений в документооборот предприятия, например, новые формы и сроки сдачи статистической и финансовой отчетности, изменение реквизитов контрагентов и т.п.

Предложенные модели на базе ИИ позволят значительно повысить уровень безопасности, снизить издержки и более рационально использовать имеющийся на предприятии трудовые ресурсы. Системы управления на базе ИИ способствует снижению правовых рисков, издержек на выплату штрафов путем комплексной проверки и выделения с последующим отсеиванием «токсичных» связей и контрагентов. Кроме того, контроль за соблюдением технологических процессов может снизить уровень брака и травматизма на производстве, избежать потерь рабочего времени [89].

Методы защиты информации от кибератак на уровне пользователей сетей организации. Для предупреждения большинства кибератак на уровне менеджеров низшего и среднего звена управления необходимо соблюдать основные меры безопасности при работе в информационной среде. Для защиты от социальной инженерии предлагаются следующее:

- иметь два почтовых ящика – личный, используемый для персональной корреспонденции, и публичный, используемый для регистрации на различных порталах;
- не переходить по ссылкам в письмах, полученных от неизвестных источников;
- не отвечать на спам;
- своевременно обновлять браузер;
- использовать специальные антифишинговые и спам-фильтры при работе в Интернете.

Для защиты от вредоносного ПО необходимы следующие мероприятия:

- установить современные антивирусные программы;
- постоянно обновлять ПО устройства до максимальной версии потому, что зачастую злоумышленники используют уязвимости в устаревшем коде, вследствие чего разработчики постоянно выявляют их и выпускают обновления [90];
- регулярно осуществлять резервное копирование всех данных, как в облачное хранилище, так и на физический носитель;
- составлять сложные пароли для учетных записей, не состоящие из общедоступной информации (дата рождения, номер телефона, ФИО), кроме того, необходима полная смена паролей от всех учетных записей не реже раза в месяц;

- в банковских и почтовых сервисах применять двухфакторную аутентификацию. Обычно в организациях более 60% инцидентов в сфере информационной безопасности связано с внутренними нарушениями.

Технологии защиты от внутренних угроз информационной безопасности подробно раскрыты в статье А.Е. Сулавко [91]. Большинство из них связано с социальной инженерией. Неосведомленный работник является потенциальным нарушителем и источником возникновения угрозы. Для предотвращения внутренних нарушений в организации необходимо внедрение специальной системы обучения и контроля знаний по информационной безопасности. Сотрудникам отдела информационной безопасности необходимо донести до работников ключевые сведения о потенциальных угрозах, выдать соответствующие информационно-справочные материалы и провести инструктаж. В настоящее время в вопросах информационной безопасности распространяется проактивная и другие виды защиты информационных ресурсов [92]. Для борьбы с киберпреступниками специалистам необходимо опережать хакеров по уровню знаний, разрабатывать превентивные методы защиты программного обеспечения, заранее искать и устранять потенциальные уязвимости в защищаемых системах.

Рассмотрение проблем защиты информации с позиций системного подхода приобретает важное значение, как в плане теории познания, так и с практической точки зрения. В методологическом отношении исследование информационной безопасности предприятия как системы дает о ней, прежде всего, целостное представление, что, в свою очередь, позволяет с большей достоверностью и обоснованностью определять практические меры по ее обеспечению в целом и в различных конкретных условиях. Содержание «теоретико-технологических» мероприятий информационной безопасности предприятия представляет собой обоснование объективной необходимости и определение частных и общих задач защиты; разработку соответствующих правовых, экономических, организационных, технических, социальных и других норм ее осуществления; проведение анализа правонарушений в различных информационных сферах; исследование состояния и перспектив развития средств, методов и форм организации, планирования, контроля и непосредственного осуществления защиты информации. Исследование и анализ различных сторон практической деятельности ведущих западных и российских фирм, специальных государственных и частных служб и других организаторов и исполнителей функций обеспечения безопасности ИС показывает, что системный подход к решению проблемы защиты информации не только полезен в реальной практической деятельности, но является единственным правильным направлением достижения надежной информационной защиты.

2.6. Методы повышения эффективности экономической защиты

Несмотря на продолжающиеся международные конфликты, угроза крупномасштабного вооруженного конфликта постепенно отходит на второй план. Наличие у России мощного оборонно-промышленного комплекса, производящего высококлассные системы вооружений, а также обладание ядерным оружием и средствами его доставки практически нивелирует силовое разрешение каких-либо конфликтов. Именно поэтому в отношении России ведется война другого характера – экономическая и финансовая и противостоять агрессии такого рода может сильная экономика, обладающая серьезным инновационным потенциалом. В настоящее время Россия сталкивается с беспрецедентным давлением со стороны ряда индустриально развитых стран, заключающиеся в ограничениях на закупку высокотехнологичного оборудования, приборов, материалов и др. [93]. В настоящее время, предприятия оборонно-промышленного комплекса остались практически единственными источниками научно-технической информации и технологических знаний. Процесс передачи научно-технической информации и технологий в гражданский сектор экономики является на современном этапе одним из самых важных и заслуживающего особого внимания.

Конверсия представляет собой управляемый процесс реализации проектов по выпуску продукции гражданского или двойного назначения предприятиями оборонно-промышленного комплекса [94]. Предприятия оборонно-промышленного комплекса (ОПК), куда входит ракетно-космическая и авиационная промышленность, располагает уникальным оборудованием и технологиями, которые можно использовать для производства продукции гражданского назначения. Среди множества различных вариантов использования военных технологий в гражданской сфере экономики, конверсия авиационно-ракетной техники представляется наиболее логичным и эффективным решением проблем финансирования инновационного процесса. Первая волна конверсии отечественного ОПК началась практически сразу после окончания Великой Отечественной войны. Предприятия, выпускавшие ранее вооружения, обмундирование, амуницию и военную технику достаточно быстро перешли на выпуск гражданской продукции. В авиации появились гражданские самолеты на базе дальних бомбардировщиков, к числу которых относится первый в мире реактивный пассажирский самолет Ту-104. Построенный на базе дальнего бомбардировщика Ту-16, гражданский самолет в течение двух лет был единственным в мире реактивным пассажирским авиалайнером. Конструкторские и технологические работы начались с постановления Совета Министров СССР от 11 июня 1954 г., а уже через год – 17 июня 1955 г. Ту-104 совершил свой первый

полет. После испытаний и доработок отдельных узлов и агрегатов, в 1956 г. самолет поступил в серийное производство и вышел на внутренние регулярные рейсы. На международных авиалиниях в 1957 г. Ту-104 выполнял рейсы в Прагу, Лондон Дели, Оттаву и другие города мира. Распространение инновационной техники шло высокими темпами. Выпуск самолетов в течение двух лет был налажен на трех авиационных заводах, расположенных в Харькове, Казани и Омске. Другим конверсионным самолетом стал турбовинтовой Ту-114, переделанный из дальнего бомбардировщика Ту-95. Работы по проектированию начались в 1955 г., первый полет состоялся в 1957 г., регулярные рейсы начались в 1961 г. Пассажирский самолет Ту-114 в то время считался самым большим и самым быстрым среди турбовинтовых авиалайнеров в мире. Успешными оказались проекты по созданию гражданского транспортного самолета Ил-76ТД-90А на базе военного Ил-76, а также вертолетов МИ-8 и Ми-26, которые успешно применялись не только военных целях, но и в народном хозяйстве.

В ракетостроении достаточно близкими оказались военное и гражданское направления. Баллистическая ракета Р7 проектировалась изначально как боевая и предназначалась для доставки ядерных боеприпасов на значительные расстояния. После модернизации баллистическая ракета стала использоваться в качестве ракеты-носителя для вывода на околоземную орбиту космических аппаратов. Можно отметить, что гражданская техника создавалась на предприятиях ОПК параллельно с военной, а начальный этап инновационного цикла составлял от двух лет в авиации до 4-х лет в ракетостроении. Благодаря особенностям административно-командной системы, обеспечивающей вполне эффективный контроль за использованием ресурсов, страна смогла в достаточно короткий срок занять лидирующие позиции в высокотехнологичных секторах мировой экономики. Среди факторов, способствовавших успеху, следует отметить военную дисциплину на стратегических объектах и серьезную персональную ответственность за соответствующее выполнение плановых заданий руководителей всех уровней управления.

Рыночные реформы дали возможность предприятиям свободно распоряжаться своими ресурсами и капитал стал смещаться в те сектора экономики, в которых были созданы условия для получения максимального дохода с минимальными рисками. В результате наукоемкие предприятия довольно быстро лишились инвестиций и квалифицированных кадров. Практически во всех учебных заведениях России были открыты факультеты, кафедры и курсы для подготовки специалистов в сфере торговли, финансов, юриспруденции, управления в ущерб инженерным специальностям. Таким образом, к началу вступления мировой экономики в шестой технологический уклад, наукоёмкий сектор российской экономики оказал-

ся практически без финансирования, без квалифицированных кадров, с отсталой материально-технической базой и с колоссальной задолженностью перед банками и другими финансовыми структурами. Многие предприятия базовых отраслей промышленности были разорены и поглощены иностранными корпорациями или перепрофилированы в торгово-развлекательные, складские и офисные центры.

В результате тотальной приватизации ряд стратегически важных для экономики России предприятий был раздроблен, разорваны сложившиеся научно-производственные связи. Многие предприятия уже не могли выполнить поставленные задачи, и вынуждены были ориентироваться на закупку зарубежного оборудования, материалов и комплектующих [95].

Одними из немногих выживших предприятий наукоемкого сектора экономики были научные организации и производства, входившие в ОПК, и игнорировать потенциал которых в современных условиях, было бы нерационально.

Авторы рассматривают отечественный ОПК как один из важнейших элементов поддержки инновационной активности предприятий и организаций различных форм собственности и видов экономической деятельности.

Предприятия ОПК могут выступать как в роли технологического донора, так и в качестве заказчика услуг, материалов и комплектующих, необходимых для выпуска вооружений и продукции гражданского и двойного назначения.

Необходимым условием существования любого предприятия является спрос на его продукцию или услуги. Наличие у гражданской организации долгосрочного контракта с предприятием ОПК однозначно повышает ее инвестиционную привлекательность и способствует притоку квалифицированных специалистов. Эти факторы значительно повышают вероятность качественно и в срок выполнить условия контракта с предприятием ОПК.

Положительным моментом является и то обстоятельство, что частные компании проводят исследования и разработки самостоятельно или заказывая проведение НИР у научно-исследовательских организаций. В этом случае экономят бюджетные средства, направляемые на финансирование прикладных исследований. Гарантируя частной компании сбыт продукции и услуг предприятиям ОПК, государство может оказать существенную поддержку малому и среднему бизнесу, задействованному в реализации государственного оборонного заказа (ГОЗ). Включенные в орбиту ГОЗ, предприятия приобретают столь необходимую в кризисных условиях финансовую устойчивость. Основной продукцией, в достаточно больших объемах потребляемой предприятиями ОПК, являются различные конструкционные и лакокрасочные материалы, электронные приборы, микросхемы и другая элементная база, транспортные средства, двигатели, электрические машины и др. Гос-

ударственная поддержка малому и среднему бизнесу может быть реализована посредством закупки определенного вида услуг для Вооруженных сил. К числу высокотехнологичных услуг, которые могут оказывать частные компании различным государственным структурам, можно отнести связь, информационные и транспортные услуги, ремонт и обслуживание техники, зданий и сооружений и др.

Особое место здесь занимают информационные услуги, в которые входят наблюдение за земной поверхностью, метеорологические прогнозы, мониторинг социальных сетей, интернет-ресурсов, социологические исследования и др.

За рубежом военные и другие государственные структуры достаточно широко сотрудничают с частными компаниями, предоставляющими услуги космической связи и дистанционного зондирования Земли (ДЗЗ) [96]. Специфика блока НАТО состоит в том, что военные базы, расположенные на всех континентах планеты и находящиеся в плавании корабли военно-морского флота, нуждаются в устойчивой связи с командными центрами и друг другом. Для обеспечения надежного взаимодействия между подразделениями, правительствами ряда стран и руководством блока было решено привлечь частные компании к организации надежной и устойчивой связи. Кроме того, было принято решение о возможности использования информации с коммерческих спутников ДЗЗ. Таким образом, посредством гарантированного контракта, государством была оказана поддержка частным предприятиям-изготовителям и разработчикам ИСЗ и фирмам-операторам связи и мониторинга земной поверхности.

Взаимосвязи между частными компаниями, государственными структурами и предприятиями ОПК сформулированы в модели спроса, гарантированного государством (рис. 5).

Характерной особенностью модели является перетекание гражданских технологий в ОПК, что значительно повышает эффективность использования бюджетных средств.

Одним из недостатков предложенной модели может являться угроза утечки секретной информации с гражданских объектов, связанных с оборонной промышленностью и непосредственно с силовыми структурами. Следует учитывать и то обстоятельство, что на стабильность спроса со стороны государства оказывает влияние множество внутренних и внешних факторов, к числу которых относятся военно-политическая обстановка в мире, состояние бюджета, ситуация на мировых финансовых рынках и т.д. Чтобы иметь возможность выполнить условия контракта, предприятие должно обладать передовым научно-промышленным потенциалом и устойчивыми связями с поставщиками услуг, материалов и комплектующих [97].

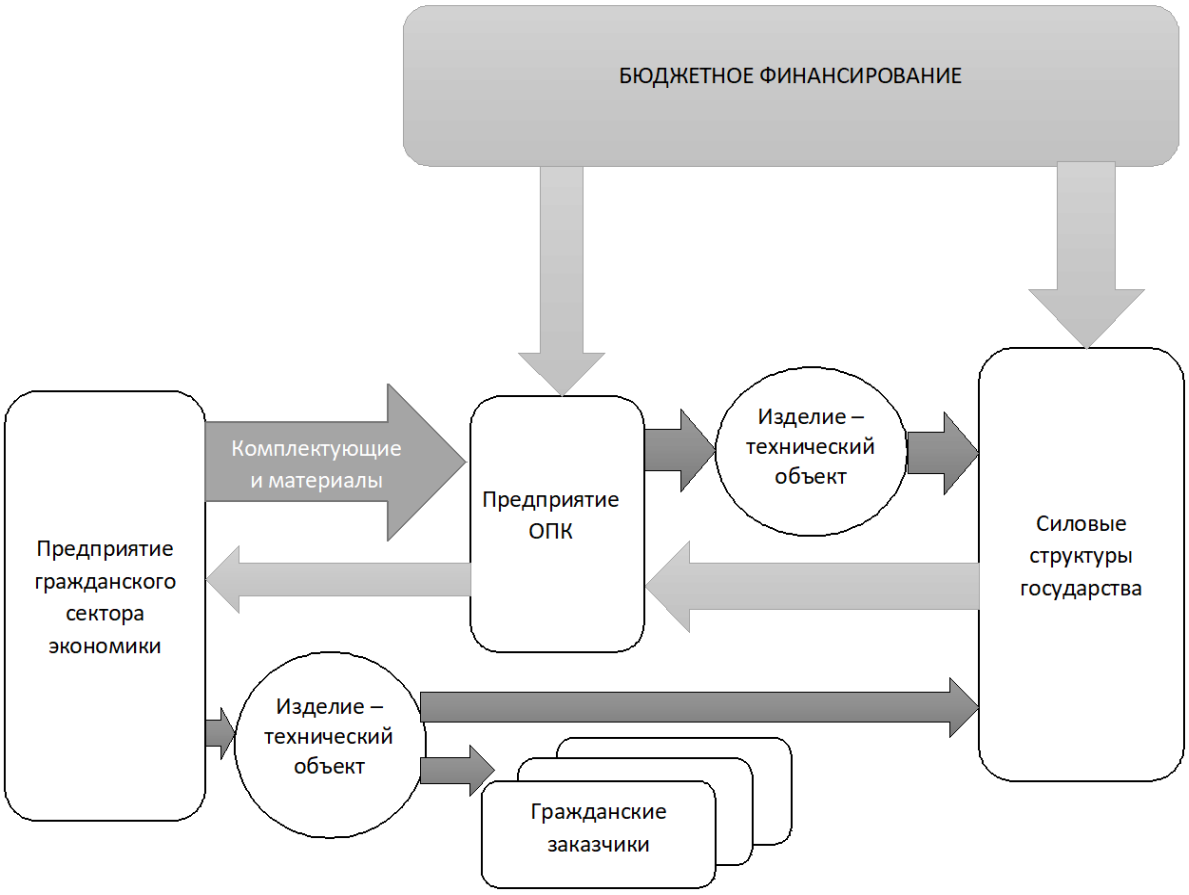

Рис. 5. Модель гарантированного спроса (темным цветом обозначены материальные потоки, светлым – финансовые) [99]

Особенностями функционирования наукоемких производств, входящих в ОПК, является их закрытость, в результате чего, передовые технологии, разработанные на средства бюджета, как правило, применяются на одном предприятии и не известны другим предприятиям, входящим в ОПК, не говоря о гражданском секторе экономики. В современных условиях ускорения инновационного развития, большое значение имеют темпы распространения новых видов продуктов, технологий и методов в экономической системе. Сложившаяся ситуация не позволяет полностью раскрыть имеющийся в экономике инновационный потенциал и для решения этой проблемы необходимо решить три основные задачи. Во-первых, нужно создать информационную базу перспективных для гражданского сектора экономики технологий. Другой задачей является адаптация военных технологий в производства гражданского сектора экономики. И третья задача заключается в организации правовой и экономической защиты адаптированных инновационных технологий. Авторами предложена модель диффузии оборонных технологий в гражданский сектор экономики [99], показывающая взаимосвязи субъектов инновационной деятельности в процессе их взаимодействия друг с другом (рис. 6).

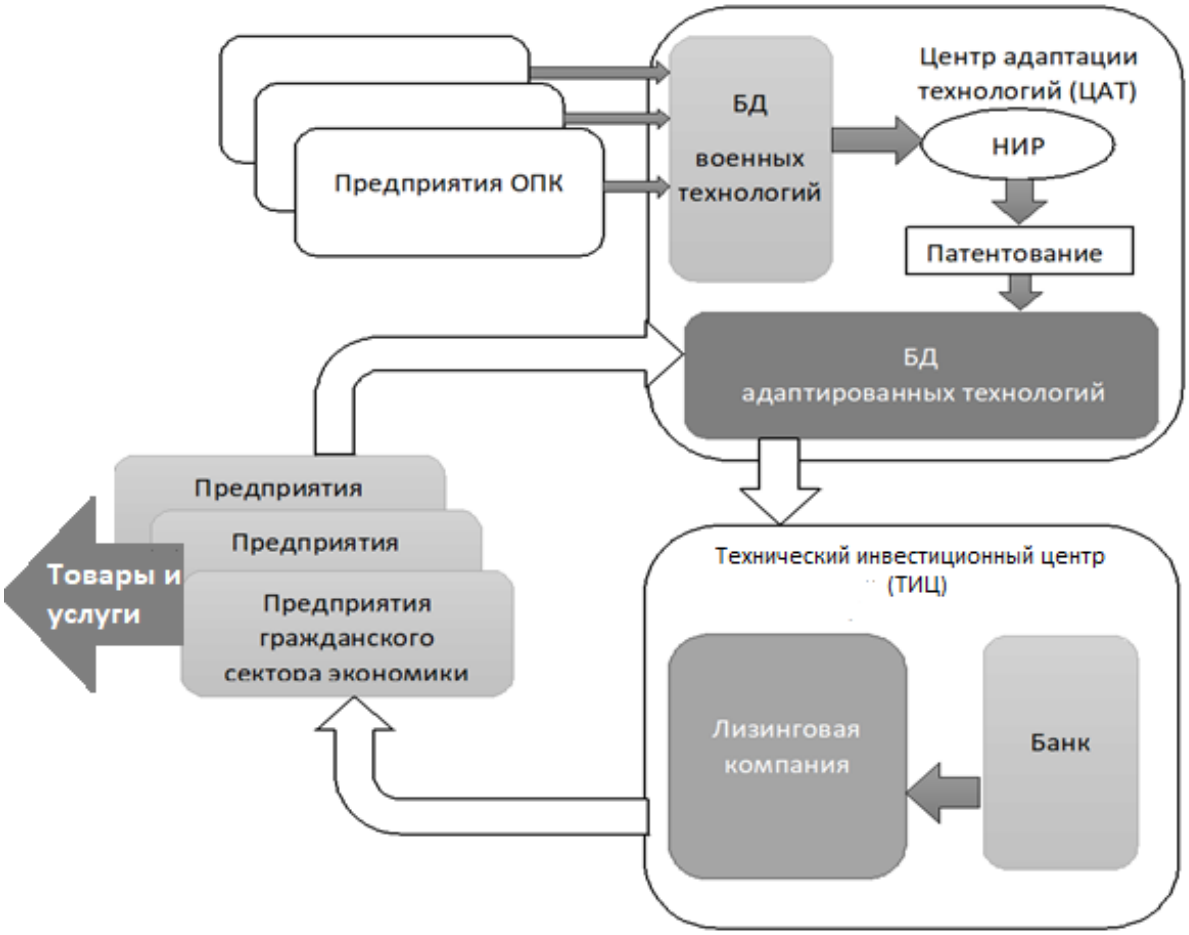

Рис. 6. Модель диффузии технологий ОПК в гражданский сектор экономики [99]

Ключевым элементом модели является Центр адаптации технологий (сокр. ЦАТ), в котором на первом этапе комиссия экспертов отбирает перспективные технологии и продукцию ОПК для передачи в гражданский сектор экономики. На следующем этапе специалисты центра совместно с разработчиками адаптируют технологию, ранее применявшуюся в на предприятии, входившем в состав ОПК. Полученные результаты технологических и конструкторских работ защищаются патентами и помещаются в информационную базу адаптированных к гражданскому сектору экономики технологий ОПК (сокр. БАТ).

В функции технического инвестиционного центра (сокр. ТИЦ) входит содействие заключению лизинговых договоров по передаче оборудования и документации.

Авторы предлагают строить систему управления базами технологий на основе методологии управления жизненным циклом информации (англ. Information Life-cycle Management – ILM) [98], основанную на том, что наиболее актуальная научно-техническая информация должна автоматически перемещаться в приоритетную, максимально быструю и самую защищенный блок. Соответственно менее

важная информация перемещается на более дешевую и менее скоростную систему. Это позволит существенно экономить затраты по хранению и обработке информации и облегчит пользователю поиск [99].

Заинтересованные в новой технологии частные предприятия, совместно с разработчиками, завершают работы по технической подготовке производства для выпуска гражданской продукции.

Технически процесс передачи адаптированных технологий ОПК в гражданский сектор экономики реализуется посредством продажи лицензий или с использованием лизинговых схем.

Предлагается следующий порядок передачи технологий:

- предприятие гражданского сектора экономики осуществляет поиск и находит в БАТ подходящий объект;
- на основании запроса предприятия, специалистами ЦАТ производится совместная доработка технологии под требования заказчика;
- при содействии ТИЦ заключаются лицензионные соглашения и лизинговые контракты;
- предприятие оплачивает и получает и необходимую техническую документацию, оборудование, кредиты на освоение новой технологии и выпуск новой продукции.
- Лицензионные соглашения должны предусматривать платежи в форме роялти с субсидированием предприятию части его расходов по приобретению лицензии.

Особое внимание следует уделить экономической и правовой защите инновационных проектов, на базе конверсионных технологий. В качестве экономической защиты наиболее рационально использовать страхование имущества от возможных инновационных рисков [100]. Проблемой является организация правовой защиты конверсионных технологий. Полученная по льготной цене интеллектуальная собственность может быть нелегально перепродана конкурентам или вовсе уйти за рубеж. Частное предприятие, обладающее новыми конверсионными технологиями может быть искусственно поставлено на грань банкротства и приобретено вместе с имеющимися у него патентами иностранными транснациональными корпорациями. Чтобы этого не произошло, должны быть установлены ограничения на все слияния и поглощения на срок действия конверсионной технологической лицензии.

Анализ показывает высокую эффективность использования военных технологий в гражданском секторе экономики по сравнению с созданием новых граж-

данских технических объектов. Конверсионные проекты требуют для своей реализации гораздо меньше времени и ресурсов.

В настоящее время имеется достаточно примеров успешной реализации проектов конверсии военных технологий, среди которых особое внимание следует обратить на модернизацию баллистических ракет, на базе которых было создано несколько ракет – носителей разного класса, среди которых Рокот и Днепр. Работы по созданию ракет-носителей были начаты в начале 90-х годов и, не смотря на разрушительные для космической отрасли последствия реформ, всего через восемь лет начались полеты конверсионных ракет с коммерческой нагрузкой на борту, в то время как работы по проектированию и испытанию новой ракеты-носителя «Ангара» еще полностью не завершены [99]. Аналогичная ситуация наблюдается и с авиационной техникой. Конверсионные самолеты Туполева уже через год поднимались в небо, в то время, как отечественные разработки самолетов МС-21 и SSJ-100 продолжались десятилетиями.

В настоящее время гражданский сектор экономики успешно использует множество видов техники и услуг, которые изначально проектировались для военных целей. Система глобальной навигации ГЛОНАСС, спутниковая связь, системы мониторинга и зондирования земной поверхности и мирового океана и многое другое. Отечественные предприятия ОПК обладают внушительным потенциалом в сфере технологии обработки и получения новых материалов, технических решений в области энергетики, транспортных средств, наблюдения, связи и др., который пока не используется в гражданском секторе экономики. Задача конверсии – сделать доступными для широкого круга потребителей новые технические решения без ущерба безопасности страны. Предложенные в данной работе подходы к распространению технологий ОПК в гражданский сектор экономики позволят снизить бюджетные расходы и повысить устойчивость экономической системы к внешнему воздействию. Кроме того, ожидается снижение импортозависимости за счет притока на местные рынки товаров и услуг высокого качества отечественного производства. Предложения по созданию Центра адаптации технологий позволит малому и среднему бизнесу, не обладающему достаточными ресурсами для производства высокотехнологичной продукции приобрести современное оборудование, техническую документацию и финансирование в необходимом объеме. Разработанная в данной работе модель диффузии технологий ОПК в гражданский сектор экономики дает возможность контролировать материальные и финансовые потоки, возникающие в конверсионных процессах.

В целом, разработанный авторами механизм конверсии технологий ОПК должен способствовать повышению эффективности бюджетных расходов, сниже-

нию импортозависимости и, тем самым, повышением уровня безопасности экономической системы.

2.7. Подходы к противодействию нелегальному финансированию бизнеса и коррупции

Созданный в 2002 г. Комитет Российской Федерации по финансовому мониторингу, в дальнейшем Федеральная служба по финансовому мониторингу (Росфинмониторинг) совместно с Центральным Банком России провели ряд эффективных мероприятий по пресечению нелегального оттока капиталов [101], однако в посткризисный период 2008–2010 гг. столкнулись с новой проблемой – схемы с применением криптовалюты.

Криптовалюты – это электронные деньги или цифровые активы, которые создаются частными компьютерными системами без контроля центральных банков. Самая известная криптовалюта на сегодняшний день – биткоин. Целью создания данной системы было введение в оборот нового средства платежа, при помощи которого его обладатели смогут обменивать добытые ими биткоины на товары и услуги. Продавцы этих товаров и услуг согласны принимать биткоины к оплате, потому что уверены в том, что в будущем также смогут тратить полученные ими биткоины на другие товары и услуги. То есть изначально биткоины создавался как альтернативная валюта. Как и другие современные валюты, биткоин не обеспечен реальными активами, а основан на доверии сторон, принимающих его в качестве оплаты.

На текущий момент Минфин РФ против жесткого запрета криптовалюты. Однако, согласно законодательству России, все товары и услуги должны продаваться в рублях. То есть на территории России нельзя деноминировать товары и услуги в другой валюте. Парадокс, сложившийся ситуации заключается в том, что торговые сделки в биткоинах считаются нелегальными, а генерировать криптовалюту можно [102].

Возникает проблема, как максимально эффективно использовать инновационные финансовые инструменты и информационные технологии в развитии экономики России и полноценно интегрироваться в мировое финансовое пространство, не упуская возникающих возможностей [103]. И, в тоже время, как ограничить свободу мошенников, которые используют биткоины в нелегальных транзакциях. Кроме того, нельзя забывать и про возможное финансирование терроризма с помощью цифровых денег. Следовательно, необходимо дополнительное обоснова-

ние введения ответственности за выпуск и оборот криптовалют, определение критериев степени их общественной опасности.

В этой связи стоит рассмотреть возможности адаптации зарубежного опыта в области развития инструментов финансового мониторинга, базирующегося на риск-ориентированном подходе, путем:

1) контроля внедряемых в повседневную практику финансово-информационных инноваций, с целью пресечения отмывания незаконных доходов и финансирования терроризма;

2) выработки мер по оценке и минимизации новых угроз, связанных с развитием научно-технического прогресса в платежных системах (криптовалюты, биткоины, предоплаченные карты).

Сейчас Государственная служба оценка рисков отмывания денег и финансирования терроризма в Великобритании (англ. – *UK National risk assessment of money laundering and terrorist financing*) присуждает цифровым деньгам нижний класс опасности в связи с их сложной процедурой быть украденными, переданными другими лицам и другим причинам. Тем не менее, считать это мнение оправданным не представляется возможным в силу отсутствия полноценной статистики по таким случаям, т.е. использования цифровых валют в криминальных целях [104].

Рассмотрим отношение к криптовалютам Financial Crimes Enforcement Network (Система борьбы с финансовыми преступлениями США) [105].

FinCEN дает такое определение криптовалютам: «виртуальная валюта – средство обмена, которое работает как обычная валюта в некоторых средах, но не имеет всех признаков реальной валюты. В частности, у виртуальной валюты нет статуса законного тендера ни в какой юрисдикции».

Поскольку криптовалюты не существуют в форме банкнот или монет, нет возможности оплатить ими мелкие повседневные услуги или продукты. Они только существуют как ряды цифровых символов. Для использования виртуальной валюты нужно открыть счет в одном или нескольких электронных кошельков. Для других пользователей идентификация того, кто владелец, состоит только из адреса электронной почты поддающегося проверке (но при этом существует множество анонимных почтовых услуг), и в некоторых случаях телефона, с которого можно посылать сообщения или получить их (и который может быть анонимным заранее купленным телефоном). Платежи можно осуществлять в банке, который конвертирует реальную валюту в виртуальную, которую можно переслать в другой кошелек любую точку планеты. Виртуальную валюту можно потом обменять на валюту любой другой страны. Таким образом, необходим только адрес пользователя биткоина, чтобы провести финансовую операцию, которая не содержит информации об идентифика-

ции. Операция с биткоинами, принимает форму трансфера между биткоиновскими кошельками и будет зарегистрирована в специальной структуре для записи группы транзакций, названной «blockchain» [106].

Заметим, что особенности криптовалют могут стать привлекательны для нелегального движения капитала в силу их:

- анонимности криптовалют;
- глобального распространения;
- мгновенности транзакции;
- невозможности отказа от выполнения обязательств;
- низкой стоимости транзакций;
- простоты использования;
- постоянного повышения технических стандартов безопасности и анонимности;
- практической невозможности государственного мониторинга транзакций;
- возможности смены адресов регистрации транзакций.

Однако преувеличивать опасность цифровых валют несколько преждевременно, так как:

- курс криптовалют к официальным деньгам изменяется стремительно и непредсказуемо;
- онлайн-кошелек может стать мишенью для хакеров и воров;
- ещё не отработаны схемы конвертации денег в криптовалюты и их обмен на товары организациями, которым пользователи могут «доверять»;
- возрастающий интерес государств к мониторингу криптовалют.

Виртуальные валюты представляют собой реальную и находящуюся на стадии становления проблему для всего международного сообщества в части разработки инструментов обнаружения и предотвращения нелегального движения капиталов. К настоящему времени заинтересованные страны проявляют разные подходы к этой проблеме. Некоторые по существу запретили их использование. Другие начали интегрировать виртуальные валюты в существующие регулирующие режимы.

Следующие рекомендации помогут Федеральной службе по финансовому мониторингу решать эту существующую проблему:

1. Обновить рабочую группу по контролю за финансовыми операциями новыми специалистами в области исследования криптовалют.

2. Мотивировать развитие национальных (и международных) саморегулирующих организаций – это способ сбалансировать коммерческую возможность

виртуальных валют с их потенциалом для злоупотреблений. Идея состоит в том, чтобы создать неправительственные, саморегулирующие организации, наделенные правом наблюдать за виртуальными валютными операциями в национальной юрисдикции. Саморегулирующие организации обеспечили бы независимость от правительственного контроля, при этом предусматривая защиту прав потребителей и транзакционную целостность.

3. Повышать уровень сотрудничества и обмена знаниями и навыками между бизнесом, агентствами и организациями, ответственными за операции по борьбе с отмыванием денег и запрет терроризма.

4. Расширять диапазон законодательных актов, которые помогут в судебном преследовании правонарушителей – иногда проще доказать такое экономическое преступление как отмывание денег в соответствии с существующими законами, чем непосредственно доказать, что фонды использовались для незаконного перевода средств за рубеж.

5. Поддерживать бдительность относительно направлений дальнейшего развития виртуальных валют.

Предложенные меры позволят стабилизировать рынок ценных бумаг и валютный рынок в России и повысят эффективность проводимых Правительством антикризисных мероприятий [107].

ЗАКЛЮЧЕНИЕ

Современные условия нельзя назвать благоприятными для России и ее союзников. Страна находится в состоянии особого рода конфликта, который направлен уже не на сдерживание ее развития, а на уничтожение России как самостоятельной социально-экономической системы посредством экономического, социально-культурного и военного давления. Положение осложняется еще и тем, что практически все международные организации, такие как ОБСЕ, Международный валютный фонд, Всемирный банк, МАГАТЭ и др., имеющие возможность сгладить противоречия и остановить конфликт, находятся под контролем США и их сателлитов. Противостоять этой агрессии представляется возможным только при условии мобилизации всех имеющихся ресурсов, включая финансовые, производственные, информационные и человеческие. Россия обладает колоссальными природными ресурсами, серьезным научно-производственным потенциалом, а также в состоянии привлечь значительные трудовые ресурсы для защиты своих интересов. Проведенное исследование показало, что отдельные мероприятия по реагированию на угрозы не могут эффективно противостоять вооруженному и экономическому давлению на страну. Необходимо комплексно и системно использовать все доступные методы защиты социально-экономической системы.

Вооруженные силы должны получать ресурсы не только от оборонно-промышленного комплекса, но и от предприятий гражданского сектора экономики. В свою очередь, военные технологии должны быть адаптированы к использованию на гражданских предприятиях. Разработанная авторами модель диффузии технологий ОПК способствует повышению эффективности бюджетных расходов, снижению импортозависимости и, тем самым, повышением уровня безопасности экономической системы.

В целях повышения эффективности деятельности управляемых войсковых формирований необходимо научное обоснование планов боевой подготовки, перспектив развития систем военной техники, заказов вооружения в промышленности, обеспечении поставок материальных ресурсов, организации проведения научных исследований в вооруженных силах и координации научных исследований в оборонной промышленности. Эти планы должны быть направлены на нивелирование угроз вооруженного вторжения, которые формируются в трех средах – воздушно-космической, морской и сухопутной.

В современных условиях особое значение приобретает проблема информационной безопасности, которая решается посредством внедрения специального инженерно-технического обеспечения с использованием технологий искусственно-

го интеллекта. Использование информационных технологий в банковской сфере позволяет блокировать нелегальные денежные потоки, которые могут дестабилизировать финансовую систему страны. Контроль за финансовыми потоками существенно сократил отток капитала за рубеж, значительно снизил возможности иностранных агентов влиять на социально-экономические процессы в стране. Снижение потерь в финансовой сфере позволил увеличить поддержку социальных и оборонных программ, которые в условиях нестабильности, начинают играть все более важную роль.

В мирное время финансирование исследований и разработок в военной области стимулирует не только развитие высокотехнологичного комплекса отечественной промышленности, но и способствует созданию рабочих мест, увеличение доли мирового рынка вооружений и росту авторитета страны.

Предложенные авторами методологические подходы к формированию государственной политики в сфере национальной безопасности будут способствовать повышению устойчивости национальной экономики, росту ее инвестиционной привлекательности и экономическому подъему.

ЛИТЕРАТУРА

1. Плисецкий Д.Е. Финансовая глобализация и национальная экономическая безопасность// Финансы и кредит. 2004. № 4 (142). С. 88–99
2. Каурова Н.Н. Феномен открытости экономики с позиции угроз национальной безопасности страны // Финансы и кредит. 2013. № 22 (550). С. 41–47.
3. Попов Г.Г. Фридрих Лист и национальная экономическая безопасность: история и современность // Историко-экономические исследования. 2007. Т. 8. № 1. С. 30–50.
4. Ольшевский В.Г. Экономическая безопасность в системе национальной безопасности: история и современные проблемы // Актуальные вопросы экономических наук. 2010. № 17-1. С. 278–284.
5. Латов Ю.В. Национальная экономическая безопасность в историческом контексте // Историко-экономические исследования. 2007. Т. 8. № 1. С. 5–29
6. Батадеев В. Экономическая безопасность и система национальных резервов // Вестник Института экономики Российской академии наук. 2011. № 1. С. 255–262.
7. Городецкий А.Е. Национальный суверенитет и экономическая безопасность в условиях применения экономических санкций» // Экономическая безопасность России: проблемы и перспективы материалы II Международной научно-практической конференции. 2014. С. 21–29.
8. Перкова Д.В., Худолеев А.Н. Информационная безопасность и противодействие экстремизму в контексте реализации государственной национальной политики // Вопросы национальных и федеративных отношений. 2017. № 3 (38). С. 74–81.
9. Пасичник В.Н. Категория «Безопасность» как методологическая основа государственной политики и управления национальной безопасностью // Вестник государственного и муниципального управления. 2013. № 3. С. 11–21
10. Сенчагов В.К. Новые угрозы экономической безопасности и защита национальных интересов России // Проблемы теории и практики управления. 2013. № 10. С. 8–18.
11. Безденежных В.М., Синявский Н.Г. О социально-экономических системах высокого уровня сложности как объектах обеспечения экономической безопасности // Экономика и управление: проблемы, решения. 2018. Т. 1. № 9. С. 56–66.
12. Авдийский В.И. Безденежных В.М. Теория и методология управления рисками организаций. М.: Инфра-М, 2013. 317 с.
13. Ачасов и др. Невоенное межгосударственное противоборство в XXI веке. Технологии, политика, экономика. Коллективная монография. М.: Канцлер, 2018. 291 с.
14. Гладышевский В.Л., Горгола Е.В. Гибридная война Запада и обеспечение ресурсного противодействия сетевому сценарию для России // Национальные интересы: приоритеты и безопасность. 2017. Т. 13. № 2. С. 369–383.
15. Викулов С.Ф. Эволюция противоборств. Избранное за 1988–2018 гг. М.: Канцлер, 2018. 247 с.
16. Авксентьев В.А. Этническая конфликтология в поисках научной парадигмы. Ставрополь, 2001. 268 с.
17. Доленко Д.В. Региональные конфликты в современной мировой политике // Социально-политические науки. 2011. № 1. С. 28–35.

18. Кричевский С.Ю. Международные экономические конфликты как элемент конкурентной борьбы // Менеджмент и маркетинг: опыт и проблемы: сборник научных трудов. Белорусский государственный экономический университет. Минск, 2010. С. 230–233.
19. Дериглазова Л. Асимметричный конфликт в современной американской политологии // Международные процессы. 2010. Т. 8. №2 (23). С. 29–36.
20. Аршинцева О.А. Современные международные конфликты: обзор популярных концепций// Дневник Алтайской школы политических исследований. 2011. № 27. С. 29–33.
21. Andrew Mumford. Proxy Warfare. John Wiley & Sons. 2013. 157 p.
22. Буренок В.М. Новые технологии и новые войны // Защита и безопасность. 2011. № 3. С. 8–11.
23. Галкин М.И., Трифоненков П.И. Война // Большая советская энциклопедия, т. 5. М.: Советская энциклопедия, 1971. С. 282–285.
24. Семенов М.И., Трубилин И.Т., Лойко В.И., Барановская Т.П. Архитектура компьютерных систем и сетей. М.: Финансы и статистика, 2003. 256 с.
25. Славянов А.С., Хрусталев Е.Ю. Исторические тенденции экономической глобаллизации // Политематический сетевой электронный научный журнал КубГАУ. 2017. № 9 (133). С. 882–891.
26. Хрусталев Е.Ю., Славянов А.С. Проблемы формирования инвестиционной стратегии инновационно-ориентированного экономического роста // Проблемы прогнозирования. 2011. № 3. С. 19–30.
27. Hufbauer G., Schott J., Elliott K., Oegg B. Economic Sanctions Reconsidered. Washington, DC: Peterson Institute for International Economics, 2009. 248 p.
28. Hufbauer G.C., Schott J.J., Elliott K.A. Economic Sanctions Reconsidered: History and Current Policy. Washington, D.C.: Peterson Institute for International Economic. 2009. 248 p.
29. Kholodilin K.A., Netšunajev A. (2019). Crimea and punishment: the impact of sanctions on Russian economy and economies of the euro area. Baltic Journal of Economics, Taylor & Francis, London, Vol. 19, Iss. 1, pp. 39–51. https://doi.org/10.1080/1406099X.2018.1547566
30. Гурвич Е.Т., Прилепский И.В. Влияние финансовых санкций на российскую экономику // Вопросы экономики. 2016. № 1. С. 5–35.
31. Синяков А., Ройтман А., Селезнёв С. Динамика потенциального ВВП России после нефтяного шока: роль сильного изменения относительных цен и структурных жесткостей. М.: Банк России, 2015. 53 с/
32. Омельченко А.Н., Хрусталев Е.Ю. Модель индекса интенсивности санкций на примере России / Национальные интересы: приоритеты и безопасность. 2018. Т. 14. № 1. С. 62–77.
33. Haider J.I. Sanctions and Export Deflection: Evidence from Iran // CID Working Papers 80. Center for International Development at Harvard University. 2017.

34. Dreger C., Fidrmuc J., Kholodilin K., Ulbricht D. Between the Hammer and the Anvil: The Impact of Economic Sanctions and Oil Prices on Russia's Ruble // Journal of Comparative Economics. 2016. Vol. 44. Iss. 2. P. 295–308.
35. Кокошин А.А. Стратегическая стабильность. Научно-технические, военные и политические аспекты // Вестник РАН. 2015. № 11. С. 963–970.
36. Сивков К.В. Телепортация и оружие будущего: учёные на пороге открытий, которые кардинально изменят средства и способы ведения вооружённой борьбы // Военно-промышленный курьер. 2013. № 19. С. 10–17.
37. Послание Президента Федеральному Собранию [Электронный ресурс]. URL: http://kremlin.ru/events/president/news/56957#sel=14:1:E,14:1:E
38. Стратегия инновационного развития Российской Федерации на период до 2020 года. Раздел IV Цель и задачи Стратегии. Этапы реализации. Российская газета [Электронный ресурс]. URL: https://rg.ru/pril/63/14/41/2227_strategiia.doc
39. Средний возраст и износ основных фондов обрабатывающей промышленности. Росстат. Россия в цифрах 2017. [Электронный ресурс]. URL: http://www.gks.ru/wps/wcm/connect/rosstat_main/rosstat/ru/statistics/enterprise/fund/#
40. Таможенная статистика внешней торговли / Экспорт-импорт важнейших товаров [Электронный ресурс]. URL: http://customs.ru:8111/index.php?option=com_newsfts&view=category&id=53&Itemid=1981.
41. О мерах государственной поддержки предприятий радиоэлектронной промышленности [Электронный ресурс]. URL: http://government.ru/programs/249/events/.
42. Гаврилова Е.А. Исследование методов обнаружения сетевых атак // Научные записки молодых исследователей. 2017. № 4. С. 55–58.
43. Кувшинов Н.Е., Галяутдинов А.А. Анализ вредоносной программы WannaCry // Форум молодых ученых. 2017. № 9. С. 499–503
44. Славянов А.С., Хрусталев Е.Ю. Налоговый механизм повышения эффективности иностранных инвестиций // ЭНС. 2013. № 1 (60). С. 72–80.
45. Тихомиров Ю.А. Теория компетенции. М.: Юринформцентр, 2005. 351 с.
46. Арутюнян Г.Г., Баглай М.В. Конституционное право: энцикл. слов. М.: НОРМА, 2006. 544 с.
47. Викулов С.Ф., Хрусталев Е.Ю. Совершенствование методологии программно-целевого планирования в военно-финансовой сфере // Национальные интересы: приоритеты и безопасность. 2015. Т. 11. № 23 (308). С. 2–14.
48. Викулов С.Ф., Хрусталев Е.Ю. Методология оценки и повышения эффективности оборонного потенциала государства // Политематический сетевой электронный научный журнал КубГАУ. 2015. № 4 (108). С. 533–556.
49. Викулов С.Ф. Экономика военного строительства: эволюция взглядов на проблемы, методы, решения. М.: Граница, 2013. 608 с.
50. Викулов С.Ф., Хрусталев Е.Ю. Военно-экономический анализ современных оборонных проблем России // Экономический анализ: теория и практика. 2012. № 12. С. 2–9.
51. Хрусталев Е.Ю. Оборонный потенциал России в контексте современной международной конкуренции и глобализации // Национальные интересы: приоритеты и безопасность. 2012. № 7. С. 2–14.

52. Волков А.Д. Военно-экономическая безопасность Российской Федерации // Актуальные проблемы гуманитарных и естественных наук. 2014. № 4-2. С. 28–30.
53. Воробьёв В.В. Финансово-экономическое обеспечение оборонной безопасности России: проблемы и пути решения. – С.-Пб.: ГУЭФ, 2003. – 414 с.
54. Подольский А.Г., Лавринов Г.А. К вопросу о военно-экономической эффективности использования финансовых ресурсов при планировании создания продукции военного назначения // Вооружение и экономика. 2012. № 2. С. 38–52.
55. Венедиктов А.А. Военно-экономический анализ мероприятий социального обеспечения военнослужащих // Вооружение и экономика. 2008. № 4. С. 4–11.
56. Лавринов Г.А. Состояние и тенденции развития методов военно-экономического обеспечения реализации планов развития вооружения и военной техники // Вооружение и экономика. 2012. № 4. С. 72–85.
57. Лавринов Г.А., Хрусталев Е.Ю. Методы прогнозирования цен на продукцию военного назначения // Проблемы прогнозирования. 2006. № 1. С.87–96.
58. Фарамазян Р.А. Глобализация военно-экономической деятельности // Вопросы экономических наук. 2007. № 4. С. 173–175.
59. Шавшуков В.М. Глобальный финансово-экономический кризис: причины, природа, механизмы распространения, антикризисные действия монетарных властей // Экономические науки. 2014. № 114. С. 121–125.
60. Винслав Ю.Б., Вишневская О.В. Антикризисные механизмы управления предприятием // Финансовая жизнь. 2010. № 2. С. 17–21.
61. Балаян К.Ю., Бацман А.И., Третьякова Э.В. Антикризисные инновационные стратегии в современных условиях // Modern Science. 2020. № 12-1. С. 34–40.
62. Кокшаров А. В ожидании 2010-го // Эксперт. 2009. № 28. С. 34–39.
63. Славянов А.С., Хрусталев Ю.Е. Факторный анализ внешней и внутренней среды наукоемкого предприятия на примере отечественной ракетно-космической промышленности // Политематический сетевой электронный научный журнал КубГАУ. 2017. № 8 (132). С. 742–761.
64. Славянов А.С. Проблемы формирования институциональной среды инновационного сектора российской экономики // Национальные интересы: приоритеты и безопасность. 2014 Т. 10. № 41 (278). С. 41–50.
65. Буренок В.М., Горгола Е.В., Викулов С.Ф. Национальная безопасность России в эпоху сетевых войн. М.: Граница, 2015.
66. Корчак В.Ю. Нас просто сомнут: сегодня ядерного оружия уже недостаточно для сдерживания агрессивных устремлений извне // Военно-промышленный курьер. 2013. № 19. С. 6–15.
67. Шипунов А.Г. Что лучше – покупать вооружение за границей или оснащать российскую армию отечественным вооружением? // Национальная оборона. 2013. № 2. С. 17–23.
68. Буренок В.М., Ивлев А.А., Корчак В.Ю. Программно-целевое планирование и управление созданием научно-технического задела для перспективного и нетрадиционного вооружения. М.: Граница, 2007. 357 с.

69. Лавринов Г.А., Хрусталев Е.Ю., Косенко А.А., Бабкин Г.В. Трансформация результатов фундаментальных исследований в факторы повышения обороноспособности России // Национальные интересы: приоритеты и безопасность. 2013. № 34. С. 2–9.
70. Лавринов Г.А., Хрусталев Е.Ю., Хрусталев О.Е. Фундаментальная наука как важнейший элемент современной системы обеспечения военной безопасности государства // Вестник Российской академии наук. 2017. Т. 87. № 3. С. 195–203.
71. Минкин В. И. Молекулярные компьютеры // Химия и Жизнь. 2004.№2. С. 13–17.
72. Мицек С.А., Мицек Е.Б. Экономика России в 2016 году: итоги, достижения, проблемы // Вестник Гуманитарного университета. 2017. № 3 (18). С. 6–24.
73. Зверев А.В., Сорокин А.А. Процентная политика российских банков, ее результаты и последствия для текущего экономического развития // В сборнике: Управление социально-экономическими системами и правовые исследования: теория, методология и практика Материалы международной научно-практической конференции. Брянск, 2017. С. 137–144.
74. ЦБ ужесточит требования к резервам банков при кредитовании слияний-поглощений // Ведомости от 01.02.2018 [Электронный ресурс]. URL: https://www.vedomosti.ru/finance/news/2018/02/01/749719-uzhestochit-trebovaniya
75. Барановская Т.П., Лойко В.И., Семенов М.И., Трубилин И.Т. Информационные системы и технологии в экономике. М.: Финансы и статистика, 2003. 416 с.
76. Ларин С.Н., Хрусталев Е.Ю. Использование информационных ресурсов и технологий для стимулирования инновационного развития экономики // Национальные интересы: приоритеты и безопасность. 2011. № 32. С. 2–11.
77. Авдонин Б.Н., Хрусталев Е.Ю. Методология организационно-экономического развития наукоемких производств. М.: Наука, 2010. 367 с.
78. Рыженкова О.Ю. Информационная безопасность: определение понятия, место в системе национальной безопасности // Закон и право. 2009. № 1. С. 50–52.
79. Елизарова М.И., Крупина В.А. Методология оценки экономической безопасности наукоемкого предприятия // Модели и методы инновационной экономики / Сборник научных трудов. Выпуск 7. М.: ЦЭМИ РАН, МАОН, 2015. С. 35–40.
80. Лойко В.И. Алгоритмы структуры данных ЭИС. Краснодар: КубГау, 2007. 168 с.
81. Хрусталев Е.Ю., Стрельникова И.А. Методология качественного управления инвестиционными рисками на промышленных предприятиях // Экономический анализ: теория и практика. 2011. № 4. С. 16–23.
82. Козунова С.С. Информационная система управления информационной безопасностью организации // Наука и Мир. 2016. Т. 1. № 4. С. 59–60.
83. Хрусталев Е.Ю. Экономическая безопасность наукоемкого предприятия: методы диагностики и оценки // Национальные интересы: приоритеты и безопасность. 2010. № 13. С. 51–58.
84. Kurer P. Legal and Compliance Risk. A Strategic Response to a Rising Threat for Global Business. Oxford: University Press, 2015. 215 p.
85. Положение Банка России от 2 марта 2012 г. 375-П «О требованиях к правилам внутреннего контроля кредитной организации целях противодействия легализации дохо-

дов, полученных преступным путем, и финансирования терроризма. [Электронный ресурс]. URL: https://cbr.ru/Queries/UniDbQuery/File/90134/1201
86. Дудова И.Л. Стандарты и методологичя комплаенс-контроля, управление комплаенс-рисками // Управление финансовыми рисками. 2011. № 1. С. 36–44.
87. Бухтин М.А. О комплаенс-функции и подходах к построению системы управления комплаенс и регуляторными рисками в кредитных организациях // Управление финансовыми рисками. 2019. № 4. С. 246–262.
88. Тарасова Н.В., Нестеров А.А. Механизм комплаенс-контроля в ссистеме обеспечения экономической безопасности кредитно-финансовой организации // Экономика и управление: проблемы, решения. 2020. Т. 3. № 12 (108). С. 108–114.
89. Соколов Н.А., Славянов А.С., Фешина С.С. Модели искусственного интеллекта в системе безопасности интеллектуального потенциала организации// Международный научно-исследовательский журнал. 2021. № 6-5 (108). С. 63–67.
90. Маслов Р.А. Социальная инженерия в киберинформационном пространстве и меры защиты от нее: материалы XI международной научно-практической конференции «Наука и образование: отечественный и зарубежный опыт». Белгород: ООО ГиК, 2018. С. 245–250
91. Сулавко А.Е. Технологии защиты от внутренних угроз информационной безопасности // Вестник Сибирской государственной автомобильно-дорожной академии. 2011. № 1. С. 45–51.
92. Хрусталев Е.Ю., Елизарова М.И. Концептуальные основы построения системы информационной безопасности производственного предприятия // Политематический сетевой электронный научный журнал КубГАУ. 2017. № 6 (130). С. 107–127.
93. Фешина С.С., Хрусталев Е.Ю., Славянов А.С. Проблемы ресурсного обеспечения инновационной модернизации Российской экономики // Политематический сетевой электронный научный журнал КубГАУ. 2016. № 7 (121). С. 1995–2009.
94. Ларин С.Н., Баранова Н.М., Стебеняева Т.В. Потенциал импортозамещения в ведущих отраслях экономики России // Экономика и предпринимательство. 2018. Т. 12. № 2. С. 1003–1009.
95. Ларин С.Н., Знаменская А.Н., Стебеняева Т.В. Анализ мероприятий по импортозамещению в стратегиях развития ведущих секторов российской экономики // Национальные интересы: приоритеты и безопасность. 2017. Т. 13. № 5. С. 804–813.
96. Славянов А.С., Хрусталев О.Е., Мустафина Я.М. Использование зарубежного опыта распространения космических технологий двойного назначения в целях экономии бюджетных расходов // Политематический сетевой электронный научный журнал КубГАУ. 2017. № 6 (130). С. 819–832.
97. Хрусталев Е.Ю., Хрусталев О.Е. Модельный инструментарий оценки производственной и финансовой надежности наукоемких и высокотехнологичных предприятий // Экономический анализ: теория и практика. 2017. Т. 16. № 3. С. 402–412.
98. Haeusser B.. Osuna A.. Bosman C. ILM Library: Information Lifecycle Management Best Practices Guide / International Technical Support Organization. NY. 326 p.
99. Славянов А.С., Хрусталев Е.Ю. Диффузия технологий оборонно-промышленного комплекса // Военный академический журнал. 2018. № 2 (18). С. 132–135.

100. Хрусталев Е.Ю., Славянов А.С., Хрусталев О.Е. Систематизация, классификация и методы компенсации рисков в жизненном цикле сложных наукоемких проектов на примере ракетно-космической техники // Экономический анализ: теория и практика. 2016. № 5. С. 29–40.
101. Безденежных В.М., Земсков В.В., Коновалова О.В., Николаев Д.А., Прасолов В.И., Фешина С.С. Финансовая и налоговая безопасность. М.: Инфинити, 2019. 312 с.
102. Клоков Д.В., Мосягин А.Б. Криптовалюты как финансовая составляющая теневой экономики на современном этапе // Вектор экономики. 2019. № 4 (34). С. 112.
103. Корнилов Д.А., Корнилова Е.В. Криптовалюты и токенизация бизнеса // Вестник НГИЭИ. 2019. № 5 (96). С. 107–118.
104. UK_NRA_October_2015_final_web.pdf (отчет с официального сайта https://www.gov.uk)
105. FinCEN Issues Advisory to Financial Institutions on Cyber-Events and Cyber-Enabled Crime, October 25, 2016 (с официального сайта https://www.fincen.gov)
106. Горда А.С., Горда О.С. Криптовалюты как новый элемент мировой финансовой системы // Ученые записки Крымского федерального университета имени В.И. Вернадского. Экономика и управление. 2019. Т. 5(71). № 1. С. 10–22.
107. Фешина С.С., Славянов А.С. Стабилизация рынка капитала посредством ограничения трансграничных операций с криптовалютами // Экономические исследования и разработки. 2020. № 4. С 29–37.

.

Монография

Славянов Андрей Станиславович

кандидат экономических наук, доцент кафедры
«Экономика и организация производства» МГТУ им. Н.Э Баумана

Хрусталев Евгений Юрьевич

доктор экономических наук, профессор,
главный научный сотрудник ЦЭМИ РАН

МЕТОДОЛОГИЧЕСКИЕ ПОДХОДЫ К ФОРМИРОВАНИЮ ГОСУДАРСТВЕННОЙ ПОЛИТИКИ В СФЕРЕ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ

Подписано в печать 14.11.2022 г.
Формат 60×90/16. Печ. л. 7,1. Тираж 300 экз. Заказ № 7
ФГБУН Центральный экономико-математический институт РАН
117418, Москва, Нахимовский пр., 47
Тел. 8 (499) 724-21-39
E-mail: ecr@cemi.rssi.ru
http://www.cemi.rssi.ru/

ISBN 978-5-8211-0808-1