ГАСУМЯНОВ Владислав Иванович – *доктор экономических наук, вице-президент ПАО «ГМК «Норильский никель», заведующий кафедрой корпоративной безопасности Международного института энергетической политики и дипломатии МГИМО МИД России (119454, Россия, г. Москва, пр-кт Вернадского, 76)*

КОРПОРАТИВНАЯ БЕЗОПАСНОСТЬ В СИСТЕМЕ ОБЕСПЕЧЕНИЯ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ: ТЕОРЕТИЧЕСКИЕ АСПЕКТЫ

Аннотация. *Статья посвящена некоторым аспектам развивающейся отрасли знаний, в частности обеспечению корпоративной безопасности как составной части науки о национальной безопасности. Автор рассматривает основные категории корпоративной безопасности, дает определение ряда ее понятий, излагает свое видение содержания системы обеспечения корпоративной безопасности, предлагает пути ее совершенствования.*

Ключевые слова: *безопасность, национальная безопасность, экономическая безопасность, стратегические национальные приоритеты, корпоративная безопасность, вызовы, риски, угрозы, мониторинг, оценка результатов*

Переход советской экономики административно-командного типа хозяйствования к рыночным отношениям на стыке веков привел к появлению крупных частных компаний (ЛУКОЙЛ, Сургутнефтегаз, НОВАТЭК, Северсталь, Норникель, ЕВРАЗ, Мечел и др.) с высоким объемом капитализации, в скором времени заявивших о себе как о весомой составляющей экономики Российской Федерации. Вместе с тем эти компании не имели, как правило, опыта производственной деятельности в качестве самостоятельных субъектов и были вынуждены приспосабливаться к жестким реалиям рыночных отношений, в т.ч. в области корпоративной безопасности.

При этом спектр и характер угроз, с которыми сталкивались большинство частных компаний, особенно в начальный период развития своего бизнеса, катастрофически возрастал (рейдерские захваты, мошенничества, хищения, поглощения и т.д.). Угрозы становились все более сложными, трудно предсказуемыми, подвергая опасности причинения вреда все виды предпринимательства независимо от географического расположения компаний и сферы их деятельности.

Складывающаяся десятилетиями во времена СССР система безопасности государственных предприятий не могла в полной мере удовлетворять потребности частного бизнеса в этой области, поскольку формировалась в условиях директивного централизованного государственного планирования и регулирования экономики и не предусматривала защиту интересов частного предпринимательства в той степени, в какой это требовалось для его поступательного развития.

Выстраивающиеся в постсоветский период отношения частно-государственного партнерства между бизнесом и государством, все более активное вовлечение частных компаний в крупные проекты, безусловно, предполагают участие государственных органов в обеспечении безопасности значимых для экономики России корпораций. В свою очередь, деятельность по защите частных предприятий от всевозможных вызовов и угроз также претерпевает изменения и становится неотъемлемой частью общегосударственной системы защиты национальных интересов.

Это возлагает дополнительную ответственность как на частный бизнес, так и на государство и предопределяет необходимость научного подхода к изучению, систематизации и обобщению опыта, накопленного частными предприятиями отечественного и зарубежного бизнеса, в области корпоративной безопасности и подготовки на основе исследований практических рекомендаций по совершенствованию этой работы для российских корпораций.

За последние годы российские ученые-экономисты внесли немалый вклад в теоретическое осмысление проблемы. В частности, такие исследователи, как И.С. Бусыгин, С.Б. Зайнуллин, А.В. Овчинников, К.В. Попова, В.Г. Семин, подготовили заслуживающие внимания научные труды по теме корпоративной безопасности.

Несмотря на то что в зарубежной науке корпоративная безопасность как самостоятельный предмет исследования отсутствует, в отличие от России, изучением вопросов идентификации, анализа и оценок рисков там основательно занимаются уже более 20 лет. В развитых странах Запада, и прежде всего в США, корпоративная безопасность (в нашем понимании этого направления бизнес-процесса) является составной частью риск-менеджмента и общей системы управления компанией. Особое внимание в зарубежной научной литературе уделяется проблеме отношений между бизнесом и государством.

Интересные соображения по поводу дефиниций интересов государства, которое представляют госкорпорации, и частных компаний, в т.ч. в сфере безопасности, излагает в своей книге «Страна – это не компания» (*Country Is not a Company*) лауреат Нобелевской премии 2008 г. по экономике американец Пол Кругман.

Таким образом, проблемы обеспечения корпоративной безопасности актуальны для всех хозяйствующих субъектов мирового сообщества и поэтому волнуют умы ученых и предпринимателей независимо от их национальной принадлежности.

Однако, несомненно, в более сложном положении оказываются все же российские компании, поскольку их исторический опыт в этой сфере не идет ни в какое сравнение с американским и западноевропейским.

В первые постсоветские годы своего развития частный бизнес ориентировался в основном на реактивные меры противодействия негативным внешним и внутренним факторам, которые (меры) казались в то время достаточными. Но довольно скоро руководству российских компаний с частным капиталом стало ясно, что такая стратегия обеспечения безопасности корпораций малоэффективна. С годами пришло понимание необходимости организовать в области корпоративной безопасности систематическую работу на опережение, включающую научное прогнозирование вероятного возникновения неблагоприятных условий, тенденций, вызовов, рисков и угроз, а также стратегическое планирование с целью их эффективной нейтрализации.

Функция корпораций по обеспечению своей безопасности хотя и автономна, но не существует изолированно от деятельности государства в сфере национальной безопасности, которая обеспечивается проведением единой государственной политики посредством реализации скоординированных взаимосвязанных мер нормативно-правового, военного, политического, дипломатического, экономического, управленческого, организационного и иного характера, адекватных существующим и потенциальным угрозам. Принимаемые государством меры направлены также на защиту законных интересов частного предпринимательства.

И это закономерно в силу общегосударственного значения обеспечения корпоративной безопасности, поскольку деятельность российских акцио-

нерных объединений, особенно крупных компаний, играет огромную роль в отечественной экономике, а реализуемые бизнес-проекты многочисленных российских корпораций и предприятий вносят существенный вклад в создаваемый валовой внутренний продукт. На необходимость более активного использования в этом направлении потенциала частного бизнеса указывал в своих выступлениях президент РФ В.В. Путин.

Поэтому вполне правомерен вывод о том, что эффективное обеспечение корпоративной безопасности не только способствует созданию благоприятных условий для повышения конкурентоспособности и успешного функционирования каждой корпорации, но и содействует устойчивому социально-экономическому развитию РФ, обеспечению ее национальной безопасности, экономической независимости и суверенитета.

В складывающейся на сегодняшний день неблагоприятной для России международной обстановке в условиях продолжающегося политического, экономического и психологического давления на нашу страну корпоративная защита еще прочнее интегрируется в общенациональную систему безопасности и ее составную часть – экономическую безопасность как одну из основных видов национальной безопасности[1]. В первую очередь это проявляется в обеспечении безопасности предприятий, имеющих стратегическое значение для хозяйственной жизни страны.

Отрадно отметить, что, несмотря на создаваемые Западом препятствия с целью не дать российской экономике занять достойное место в мировой хозяйственной жизни, развитие и влияние отечественного бизнеса уже давно вышло на глобальный уровень. Наши национальные корпорации составляют реальную конкуренцию многим известным компаниям с многолетней историей, а по ряду направлений занимают лидирующие позиции.

Тем не менее российские реалии таковы, что отсутствие законодательной базы, регулирующей взаимоотношения правоохранительных органов и спецслужб с корпоративным сообществом в сфере обеспечения безопасности, криминальные проявления в обществе и корпоративной среде вынуждают компании решать многие проблемы обеспечения безопасности своими силами.

Солидный вклад в создание юридической основы для организации и укрепления взаимодействия государства и предпринимательского сообщества заложил федеральный закон «О государственно-частном партнерстве»[2]. Закон регулирует хозяйственные отношения между федеральными государственными структурами, органами субъектов РФ, муниципальных образований и бизнесом, устанавливает порядок заключения ими соглашений, фиксирующих сферы ответственности и обязательства каждой стороны, в т.ч. «справедливое распределение рисков». В документе определяются полномочия Российской Федерации, субъектов РФ и муниципальных образований в сфере частного партнерства, предписывается содействие защите прав и законных интересов бизнеса. Кроме того, в этом правовом акте закрепляется право предпринимателей на возмещение убытков, причиненных им в результате незаконных действий (бездействия) государственных органов, органов мест-

---

[1] В Стратегии национальной безопасности Российской Федерации, утвержденной указом Президента РФ 31.12.2015 № 683, наряду с экономической безопасностью, в качестве видов национальной безопасности указаны также государственная, общественная, информационная, экологическая, транспортная, энергетическая безопасность и безопасность личности.

[2] Федеральный закон от 13.07.2015 № 224-ФЗ «О государственно-частном партнерстве, муниципально-частном партнерстве в Российской Федерации и внесении изменений в отдельные законодательные акты Российской Федерации». Доступ: http://www.consultant.ru/document/cons_doc_LAW_182660/

ного самоуправления и (или) должностных лиц этих органов в соответствии с российским законодательством.

Корпоративная безопасность, оставаясь в понятийном смысле неизменной величиной, эволюционирует в своем содержании и приоритетах, в расстановке акцентов, сообразуясь с динамикой, направленностью и значимостью угроз и уязвимыми местами в корпоративных структурах. В процессе совершенствования корпоративной безопасности сохраняется главная цель – обеспечение устойчивого функционирования корпораций, направленное на защиту их стратегических интересов, решение долгосрочных и краткосрочных финансово-экономических задач в сложных, в т.ч. неблагоприятных, внешних и внутренних условиях.

Несмотря на непреходящую и все более возрастающую значимость проблемы корпоративной безопасности в нашей стране, ее научно-теоретической проработке уделяется, как представляется, недостаточное внимание. Как отмечалось выше, отечественные ученые все же исследовали ряд важных аспектов этой многогранной темы, например обеспечение информационной и объектовой безопасности корпораций, нормативно-правовую базу обеспечения корпоративной безопасности.

И все же, к сожалению, приходится констатировать, что до настоящего времени нет фундаментальных научно-исследовательских работ, глубоко и всесторонне освещающих основы обеспечения корпоративной безопасности и весь комплекс вопросов, составляющих ее содержание и сущность.

На наш взгляд, сейчас особенно востребованы научные труды, раскрывающие теорию и методологию государственно-частного партнерства в сфере обеспечения безопасности российских компаний, прежде всего стратегических предприятий и территорий их присутствия. Пробелы в научных знаниях могут восполнить работы, посвященные достижению нулевого уровня коррупции в деловых отношениях; новым подходам противодействия современному международному и внутреннему терроризму; борьбе с активизирующимися кибератаками на объекты инфраструктуры, производственные и технологические процессы и информационные массивы корпораций; противодействию недобросовестной конкуренции и мошенничеству; борьбе с другими экономическими преступлениями и посягательствами на жизнь и здоровье акционеров и персонала, активы, собственность, материальные и финансовые ценности и иные объекты корпораций; разработке критериев и показателей оценки состояния их защищенности, эффективности системы безопасности, механизма ее реализации и деятельности субъектов в этой сфере.

Наблюдаемая тенденция к ужесточению международного экономического порядка и обострение конкурентной борьбы на мировом и внутреннем рынках побуждает компании активизировать деятельность в сфере обеспечения своей безопасности как на теоретическом, так и на практическом уровнях. И если для защиты национальных интересов и реализации стратегических национальных приоритетов формирование многофункциональной самодостаточной системы обеспечения национальной безопасности как эффективного инструмента государственной власти в основном завершено, то применительно к бизнесу ситуация иная.

Вследствие недостаточной научно-теоретической проработки некоторых ключевых вопросов обеспечения корпоративной безопасности в опубликованных трудах, посвященных этой теме, в принятых законах и подзаконных нормативно-правовых актах в лексиконе специалистов встречаются понятия и варианты их определений, которые не всегда достаточно убедительно обос-

нованы, трактуются по-разному, неправомерно применяются как идентичные или имеют иные погрешности.

Отсутствие единообразного понимания содержания ряда категорий сказывается в той или иной степени на усвоении сущности обеспечения корпоративной безопасности и на решении отдельных практических вопросов.

Остановимся на некоторых таких понятиях, выскажем свою точку зрения по их существу, а также предложим собственное видение содержания системы обеспечения корпоративной безопасности.

Сначала рассмотрим определение ключевого понятия – феномена корпоративной безопасности.

К настоящему времени разработано несколько определений этого понятия. Авторы формулируют их по аналогии с определением научно выверенного понятия «национальная безопасность», опираясь на ключевое слово «защищенность», содержащееся в этом определении. Большинство исследователей вполне обоснованно сводят это определение к комплексу мер (мероприятий), в результате осуществления которых достигается защищенность основ существования корпораций и их интересов от внутренних и внешних угроз, позволяющая корпорациям эффективно функционировать и устойчиво развиваться.

Соглашаясь с перечнем приведенных сущностных компонентов понятия «корпоративная безопасность», предлагаем уточненное в ряде позиций определение этой категории. *Корпоративная безопасность* представляет собой состояние защищенности интересов корпораций, их стратегических планов и целевых программ, бизнес-проектов, деловой репутации и имиджа, производственного, научно-технического, технологического и кадрового потенциала от внешних и внутренних угроз, противоправных посягательств, при котором обеспечивается достижение финансово-экономических целей корпораций, их успешное функционирование и устойчивое развитие в результате реализации комплекса взаимосвязанных нормативно-правовых, организационных, управленческих, режимных, технических, физических, профилактических, пропагандистских и иных мер.

Нужно признать, что предлагаемое определение понятия «корпоративная безопасность», в свою очередь, также не безупречно. Недостаток видится в том, что этимология существительного «защищенность» имеет очевидный охранительный, оборонительный характер и невольно воспринимается как пассивная модель деятельности и, соответственно, может настраивать на такую же парадигму поведения лиц, обеспечивающих корпоративную безопасность. Но в системе ее обеспечения немалый удельный вес занимают активные, наступательные меры. Прежде всего речь идет о грамотно выстроенной информационно-аналитической и прогностической работе, позитивные результаты которой могут, в частности, способствовать предотвращению нежелательных действий недобросовестных конкурентов или срыву планов таких агрессивных незаконных акций, как рейдерские захваты и пр.

Своевременное получение подобного рода информации представляет собой чрезвычайную ценность с точки зрения обеспечения корпоративной безопасности, поскольку на основе сведений такого характера удается принимать не только предупредительные, защитные меры, но и наступательные.

Предвосхитить нежелательные шаги партнеров и конкурентов можно путем предания гласности их неблаговидных намерений или иной дискредитации (подрыва авторитета) в глазах деловых кругов посредством СМИ, в т.ч. сети Интернет. Так, в ряде случаев желательного эффекта можно достичь благодаря

заблаговременным публикациям материалов о незаконных способах конкурентной борьбы противодействующей компании.

Полагаем, определение понятия «корпоративная безопасность» будет более полным, если оно будет сопровождаться пояснениями о наступательной составляющей в комплексе мер безопасности, с помощью которых достигается «состояние защищенности».

Несколько слов о еще одной распространенной неточности, требующей внесения ясности, – о соотношении понятий «корпоративная безопасность» и «обеспечение корпоративной безопасности».

В научной литературе и в некоторых документах корпораций, находящихся в открытом доступе, можно встретить ставший привычным штамп употребления этих категорий как идентичных, взаимозаменяемых. Кстати, аналогичная ситуация наблюдается в достаточно частом применении терминов «национальная безопасность» и «обеспечение национальной безопасности» как равнозначных.

В лексиконе практиков их однопорядковое использование стало также обычным и в неофициальном употреблении вполне допустимо. Но с точки зрения теории между этими понятиями существует разница.

По нашему мнению, корпоративная безопасность – это результат деятельности корпораций, направленной на выполнение функции достижения состояния своей защищенности. Полученный результат отражает противоречивое взаимодействие и противоборство интересов корпораций с внешними и внутренними угрозами. Иными словами, корпоративную безопасность можно трактовать как результат целенаправленной деятельности корпораций по обеспечению своей безопасности.

Обеспечение корпоративной безопасности представляет собой организационную деятельность, упорядочивающую работу субъектов обеспечения корпоративной безопасности, применение необходимых средств, методов и мер для достижения состояния защищенности корпораций.

Исходя из этого, можно так сформулировать определение данного понятия: *обеспечение корпоративной безопасности* – это систематическая деятельность корпораций, направленная на достижение финансово-экономических целей, защиту интересов бизнеса, стратегических планов и целевых программ, бизнес-проектов от внутренних и внешних угроз, противоправных посягательств и эффективное противодействие им, а также на создание благоприятных условий для успешного функционирования и развития корпораций, упрочения их экономических позиций и деловой репутации в Российской Федерации и за рубежом посредством реализации комплекса мер безопасности.

Следующая проблема, требующая внимательного изучения в интересах соблюдения терминологического единообразия, – сопоставление близких, но по своей сути отличающихся друг от друга понятий – «вызовы», «риски» и «угрозы».

Нетрудно заметить, что в большинстве публикаций на тему национальной и корпоративной безопасности авторы не утруждают себя дефиницией этих категорий, нередко смешивая и отождествляя их. К тому же если об угрозах, прежде всего угрозах национальной безопасности, имеется достаточно много публикаций, содержащих их научно обоснованную классификацию, всесторонне раскрывающих источники, виды, содержание и сущность угроз, то «вызовы» и «риски» менее исследованы и часто не разграничиваются.

Правда, в последние годы активизирована научная разработка категории «риски» после предложенной президентом РФ В.В. Путиным идеи «создать полномасштабную систему прогнозирования и управления рисками». Такая

полезная для бизнеса мысль была высказана в июне 2012 г. на Петербургском международном экономическом форуме.

Существует несколько определений понятия «риск». Разберем наиболее известные из них.

Признанные официальными определения понятий «вызовы», «риск» и «угроза» содержатся в Стратегии экономической безопасности Российской Федерации на период до 2030 года[1]. Но они ориентированы исключительно на экономическую сферу.

Согласно Стратегии, *угроза экономической безопасности* представляет собой совокупность условий и факторов, создающих прямую или косвенную возможность нанесения ущерба национальным интересам Российской Федерации в экономической сфере.

Риск в области экономической безопасности – возможность нанесения ущерба национальным интересам Российской Федерации в экономической сфере в связи с реализацией угрозы экономической безопасности.

Вызовы экономической безопасности – совокупность факторов, способных при определенных условиях привести к возникновению угрозы экономической безопасности.

Из этих определений наименее удачно сформулирована трактовка понятия «риск». Согласно данному определению, риск влечет за собой непременную угрозу, которая предшествует риску. Но в действительности это не так. Риск – это потенциальное явление (феномен), которое совсем не обязательно проявит себя в виде угрозы объекту воздействия. Например, в случае принятия корпорацией исчерпывающих превентивных мер по недопущению реализации риска или при определенном благоприятном стечении обстоятельств риск может не реализоваться.

В ряде документов компаний встречается другое толкование этого понятия. *Риск* – это воздействие на цели корпорации, которое потенциально может произойти в результате текущих процессов или будущих событий.

Представляется, что недостатком этого определения является неясность цели воздействия, которое может не только нанести ущерб корпорации, но и послужить во благо ей.

Весьма убедительно звучит еще одна трактовка понятия «риск». *Риск* – это вероятность утраты хозяйствующим субъектом некоторых своих ресурсов, отсутствия прибыли или повышенных расходов в результате реализации им какой-либо деятельности.

Едва ли корректным можно считать в качестве единственной причины «утраты ресурсов», «отсутствия прибыли» и «повышения расходов» результат собственной деятельности корпораций. Совершенно очевидно, что риск может появиться и реализоваться в результате влияния внешних факторов и обстоятельств, не связанных с деятельностью хозяйствующего субъекта.

Интересна и такая интерпретация понятия «риск», предлагаемая некоторыми специалистами. *Риск* – это практическая ситуация, в которой он возникает. Сама же ситуация представляет собой сложение разнообразных обстоятельств и условий, создающих определенную обстановку в разных сферах бизнеса.

Из данного определения не видно, в положительном или в отрицательном ключе сложившаяся обстановка влияет на корпорации. Однако с точки зре-

[1] Стратегия экономической безопасности Российской Федерации на период до 2030 года. Утв. указом Президента РФ 13.05.2017 № 208. Доступ: http://www.garant.ru/products/ipo/prime/doc/71572608/

ния безопасности нас интересуют ситуации, потенциально опасные в плане возможного нанесения ущерба бизнесу.

На наш взгляд, определение понятия «риск» применительно к корпорациям можно сформулировать следующим образом: *риск* – это возможность нанесения ущерба корпорации в результате собственных корпоративных причин или воздействия неблагоприятных внешних либо внутренних факторов.

В современном мире бизнес всегда сопровождается разнообразными рисками, поскольку любая хозяйственная деятельность предпринимателей происходит в постоянно изменяющихся и нередко неблагоприятных условиях, связана со многими юридическими и физическими лицами внутри страны и за рубежом, имеющими как совпадающие экономические интересы и потребности, так, довольно часто, и прямо противоположные.

Объективные различия интересов и потребностей бизнес-структур обусловливают разные цели и способы их достижения, которые далеко не всегда приемлемы для других сторон, порождают трения, конфликты и попытки противодействия. Риск того или иного нежелательного поведения контрагентов практически в любой момент может проявиться во взаимоотношениях с ними корпораций.

Поэтому своевременное обнаружение вероятности рисков, оценка возможной величины ущерба корпорациям, выявление наиболее уязвимых мест в их деятельности вошли в разряд наиболее актуальных задач.

Многие аспекты категории «риск» исследованы именно под этим углом зрения, и их результаты отражены в публикациях или изложены в документах компаний. Менее изученным оказался вопрос повышения эффективности бизнеса путем устранения рисков или уменьшения возможностей их реализации.

Подходы целенаправленного противодействия рискам зависят от природы их происхождения.

С нашей точки зрения, природа рисков двуедина. Во-первых, происхождение рисков обусловлено внешними факторами, которые могут проявляться как на территории нашей страны, так и за рубежом, если бизнес там присутствует. Такого рода риски исходят преимущественно от конкурентов, недобросовестных партнеров, организованных преступных сообществ, террористических организаций, криминальных элементов и отдельных государств, подключившихся, например, к политике давления на нашу страну. Риски последней категории можно назвать политическими. Они обусловливаются неблагоприятными изменениями геополитической обстановки и негативно влияют на предпринимательскую деятельность.

Так, явно ощущалась направляющая рука ряда западных государств – участников санкций, когда зарубежные банки одновременно перекрыли российскому бизнесу каналы внешних долгосрочных заимствований, которые составляли немалую часть инвестиций для развития большинства отечественных компаний.

Разумеется, риск также неизбежен, если компании не предпринимают усилий для изучения особенностей законодательства, регулирующего деятельность частных предприятий в стране, где российский бизнес имеет свои интересы.

Один из эффективных способов не допустить реализации рисков такого порядка – отказаться от некоторых видов деятельности корпораций (процессов, процедур, сделок, контрактов), которые проработаны не во всех деталях, недостаточно прозрачны и тем более изначально избыточно рискованны.

Во-вторых, риски могут быть порождены деятельностью самих корпораций или возникнуть в их внутренних структурах. Возможности проявления рисков подобного вида весьма многообразны. Они могут проявиться вследствие упущений в обеспечении корпоративной безопасности, слабой технической оснащенности некоторых производственных процессов, несоблюдения техники безопасности, низкого уровня специализации персонала, ошибок в организационной работе, недостаточно выверенных стратегических или тактических решений корпораций без тщательных расчетов своих финансовых и производственных возможностей, а также учета всех известных риск-факторов. Неверные решения могут быть приняты также по причине недостаточности и неточности информации или ее неправильной оценки относительно предполагаемых партнеров по бизнесу, поставщиков, инвесторов, используемых рынков сбыта товаров и услуг, динамики рынков, реальных потребностей и платежеспособности приобретателей продукции корпораций, изменений планов и приоритетов потребителей, которые могут повлечь отказ от намеченных сделок.

Возможность возникновения рисков объективно заложена в формировании и расстановке персонала корпораций. Несмотря на практикуемую проверку кандидатов на работу в корпорации, среди них встречаются лица, которые могут совершить хищение имущества или финансовых средств, разгласить коммерческую тайну посторонним лицам (например, за вознаграждение) или совершить иные противоправные деяния.

В промышленном производстве встречается особая категория рисков, которые можно назвать отложенными рисками и которые связаны с использованием некоторыми компаниями изношенного оборудования. Это рано или поздно может привести к выходу из строя отдельных агрегатов и авариям, если не будут приняты меры по изменению такого положения.

Хотелось бы обратить внимание на один специфический риск, связанный с использованием импортной компьютерной техники и программного обеспечения. Вполне допустимая вероятность содержания вредоносных программ создает опасность сбоя работы компьютеров и возможность доступа к коммерческой закрытой информации. С целью минимизации этого риска к деятельности в сфере информационной безопасности привлекаются квалифицированные сотрудники, способные организовать надежную защиту информационных технологий.

И еще одна череда рисков, которые с большой долей вероятности дадут о себе знать в ближайшем будущем, – это риски, обусловленные интенсивным развитием цифровой экономики и робототехники. Эти инновации, несущие бесспорно огромный положительный эффект для корпораций, могут повлечь сокращение рабочих мест в компаниях, рост напряженности в трудовых коллективах в связи с вероятностью увольнения. Пока еще есть время задуматься о превентивных мерах для смягчения возможных последствий таких потенциальных рисков.

Конечно, не все риски приходится выявлять, поскольку значительная часть их очевидна. При этом собственники и руководство компаний, как правило, осведомлены о них в полной мере. Однако корпорации идут сознательно на такие риски, когда считают их приемлемыми в сопоставлении с предполагаемым достижением финансовых целей и других запланированных результатов в итоге деятельности корпораций. На профессиональном языке такие риски называются риск-аппетитом.

Исключительно в компетенции корпоративного руководства находится решение вопроса о целесообразности принять известный объем (количество)

риск-аппетита после его всестороннего осмысления, взвешивания всех «за» и «против» или отказаться от него, если не просматривается достижение оптимального баланса между риском и успехом с реальной перспективой перевешивания баланса в сторону успеха.

Систематизация, оценка и всесторонние расчеты относительно допустимости риск-аппетита, а также прогнозирование и управление рисками возлагаются на риск-менеджмент, который осуществляет текущую работу такого плана в ходе бизнес-процесса. Службы безопасности корпораций могли бы, пожалуй, принять участие в отслеживании опасного роста уровня риска, который способен повлечь реальную угрозу нанесения недопустимого ущерба корпорациям.

Одним из важнейших ресурсов выявления и оценки вызовов, рисков и угроз является информационно-аналитическая работа, основывающаяся на современных технологиях и научных методах познания – экстраполяции, экспертном построении гипотез, моделировании будущих ситуаций, обработке статистических данных посредством математических методов, логико-интуитивном анализе и синтезе, индивидуальных и коллективных оценках.

Наиболее весомым результатом информационно-аналитической работы является выводная информация, содержащая оценку условий и факторов, формирующих внутренние и внешние вызовы, риски и угрозы деятельности корпораций, служащая базой для прогнозирования вероятного их возникновения и динамики развития с целью разработки превентивных мер по нейтрализации или снижению негативного воздействия. Например, целенаправленный сбор, систематизация и аналитическая обработка информации позволяют в ряде случаев предвосхитить насильственные слияния и поглощения корпораций посредством своевременного принятия адекватных мер противодействия.

Решение задачи более эффективного информационно-аналитического обеспечения осложняется рядом трудностей. Во-первых, наличием колоссальных объемов разрозненной, разнохарактерной и в ряде случаев противоречивой информации из массы различных источников. Из огромных потоков информации далеко не просто отбирать и систематизировать необходимые сведения для нужд обеспечения корпоративной безопасности и аналитически их обрабатывать. Во-вторых, разобщенностью информационных ресурсов корпораций и информационной несовместимостью баз данных, имеющих различные рубрикаторы и классификаторы. В-третьих, пока не решенной задачей подключения информационных ресурсов корпораций к государственным информационным ресурсам.

Преодоление этих трудностей стало возможным в ближайшей перспективе в связи с учреждением Федеральной информационной системы стратегического планирования. Система интегрирует распределенную информацию, содержащуюся в федеральных, региональных и муниципальных ресурсах и системах; данные официальной государственной статистики; информационно-аналитические материалы Российской академии наук о состоянии и тенденциях развития мировой и отечественной экономики; информацию российских представительств за рубежом о политических, экономических и других процессах в иностранных государствах, затрагивающих национальные интересы России; материалы СМИ, освещающие проблемы отечественной экономики и состояние бизнеса в других странах.

Предполагается не только механическое подключение информационных систем корпораций, прежде всего их ситуационных центров, к Федеральной информационной системе, но и внедрение новейших технологий и программ,

позволяющих корпорациям немедленно получать в автоматическом режиме необходимые данные о вызовах, рисках и угрозах корпоративной безопасности, деструктивных процессах и факторах в нашей стране и за рубежом, которые могут нивелировать успех деятельности компаний.

И наконец, изложим свои соображения относительно варианта комплексной системы обеспечения корпоративной безопасности.

По отношению к общегосударственной системе национальной безопасности все другие системы обеспечения безопасности сфер жизнедеятельности государства и общества представляют собой подсистемы. Не составляет исключения и обеспечение экономической безопасности, реализуемое посредством своей подсистемы. Ее составной частью является обеспечение корпоративной безопасности.

С точки зрения теории это логично. Однако на практике специалисты оперируют понятием «система» или, в более полном звучании, «комплексная система обеспечения корпоративной безопасности» применительно к корпорации или предприятию, справедливо полагая, что такая система соответствует статусу этой категории.

Взаимосвязь общегосударственной системы обеспечения национальной безопасности с другими подсистемами обусловливает общие подходы к их формированию и функционированию. Общность проявляется в определении, оценке и предотвращении вызовов, рисков и угроз, выделении объектов и субъектов обеспечения безопасности, наделении их необходимыми функциями и полномочиями, использовании апробированных методов и средств обеспечения безопасности и во многом другом.

Заимствования из арсенала наработок, применяемых в процессе обеспечения национальной безопасности, происходят только в случаях их очевидной эффективности и приемлемости для объектов корпоративной безопасности, исходя из возможности гармоничного сочетания с имеющимися собственными методами и средствами и с учетом своеобразия и особенностей обеспечения безопасности разнохарактерных объектов корпораций.

Анализ практики обеспечения корпоративной безопасности показывает, что в процессе развития рыночных отношений в РФ каждая частная компания самостоятельно и в известной мере обособленно разрабатывала комплексную систему обеспечения своей безопасности с учетом своей индивидуальности, а иногда и уникальности. И все же со временем стали формироваться в разных системах общие характерные черты и подходы, позволяющие говорить об известной унификации различных элементов систем, о появлении общей модели или типовой системы обеспечения корпоративной безопасности.

Единообразие такого порядка вовсе не означает стабильность параметров подобной типовой системы и не сковывает инициативу и креативность участников ее реализации. Типовая система обеспечения корпоративной безопасности постоянно эволюционирует, трансформируется и модернизируется в соответствии с изменяющейся обстановкой и условиями производственной и коммерческой деятельности компаний в конкретный период. Поэтому термин «типовая система обеспечения корпоративной безопасности» имеет условный характер. Структура этой системы служит лишь ориентиром для заинтересованных лиц, применяющих ее по своему усмотрению, исходя из здравого смысла и объективных возможностей корпораций.

Система обеспечения корпоративной безопасности представляет собой регулируемый нормами права механизм согласования и координации взаимодействия субъектов обеспечения корпоративной безопасности на основе соблюдения выработанных практикой принципов при разработке и

реализации комплекса взаимосвязанных мер, направленных на выявление и противодействие вызовам, рискам и угрозам корпорациям, защиту их интересов и достижение целей, эффективное функционирование и устойчивое развитие.

Система обеспечения корпоративной безопасности включает: нормативно-правовую базу; субъекты; объекты; сферы; силы, средства, методы, меры и мероприятия; мониторинг и контроль за ходом осуществления мер и мероприятий по обеспечению корпоративной безопасности, оценку результатов деятельности в этой сфере, эффективности функционирования системы и действий участников ее реализации; информационно-аналитическое, материально-техническое, финансовое, научно-методическое и кадровое обеспечение.

Нормативно-правовая база, объекты, силы, средства и методы (мероприятия) как компоненты системы обеспечения корпоративной безопасности достаточно основательно изучены, и их результаты отражены в различных публикациях. Поэтому в данной научной статье не будем заострять на них внимание. Значительно меньше материалов имеется о субъектах обеспечения корпоративной безопасности, мониторинге, контроле и оценке результатов деятельности в этой области, а сферы обеспечения корпоративной безопасности смешаны с объектами.

Попытаемся вкратце осветить эти вопросы.

Анализ научных работ и доступных материалов по обеспечению корпоративной безопасности показывает, что перечень субъектов такой деятельности неполон. В него обычно включаются: собственники, акционеры, руководство и топ-менеджеры корпораций, а также сотрудники подразделений безопасности. Вне поля зрения остаются: работники кадровых подразделений, осуществляющие набор и проверку кандидатов на работу в корпорации; персонал научных (где они имеются) и информационно-аналитических подразделений; государственные институты обеспечения национальной безопасности, которые содействуют достижению состояния защищенности корпораций; общественные организации (частные сыскные и охранные службы, ведомственная охрана государственных органов, юридические организации), принимающие участие в обеспечении национальной безопасности и привлекаемые к обеспечению корпоративной безопасности.

Наверное, имеет практический смысл выделить сферы обеспечения корпоративной безопасности в качестве самостоятельного компонента системы в силу их отличий от объектов по своему содержанию и сущности.

К сферам обеспечения корпоративной безопасности можно отнести:

– человеческий капитал (персонал предприятий);

– информационную структуру;

– логистику (производственную, транспортную, запасов, сырья, закупочную, складскую);

– интеллектуальную собственность;

– бизнес-интересы корпораций;

– стратегии развития, стратегические и краткосрочные планы и целевые программы обеспечения безопасности корпораций;

– бизнес-проекты.

Эффективность системы обеспечения корпоративной безопасности компании определяется проверкой функционирования ее составных компонентов, прежде всего такого звена системы, как реализация мер и мероприятий, содержащихся в инструкциях, режимных документах, планах и целевых программах. Для решения такой задачи выработана специфическая триада, состоящая

из процедур мониторинга, контроля и оценки хода и результатов осуществления защитных мер и мероприятий. Все три процедуры лишь относительно самостоятельны, поскольку неразрывно связаны между собой и образуют, по сути, единый процесс.

Формулировка *мониторинга* может быть следующей: это специально организованное непрерывное наблюдение за процессами и итогами проведения мер и мероприятий, предназначенных обеспечивать защищенность корпораций, а также отслеживание результатов деятельности и взаимодействия между субъектами обеспечения корпоративной безопасности.

Термин «контроль» несет вполне понятную смысловую нагрузку и не нуждается в уточнении.

Важно организовать мониторинг и контроль таким образом, чтобы их функции не ограничивались только фиксацией позитивных и негативных явлений в обеспечении корпоративной безопасности. Активная составляющая мониторинга и контроля заключается в анализе объективной информации, собираемой ситуационными центрами корпораций, сотрудниками служб безопасности, персоналом кадровых, информационно-аналитических и научных подразделений. Особый интерес проявляется к материалам о причинах, факторах и условиях, которые отрицательно влияют на состояние защищенности корпораций. Результаты такой работы дают необходимый эффект, если полученная информация незамедлительно доводится до руководства корпораций и побуждает его оперативно вмешиваться в случае необходимости в действия тех или иных субъектов обеспечения корпоративной безопасности или принимать меры к устранению обнаруженных недостатков в отдельных звеньях системы обеспечения корпоративной безопасности.

Весьма сложной и пока не полностью отработанной процедурой является оценка хода и итогов осуществления защитных мер и мероприятий. В подразделениях безопасности, в компетенцию которых входит определение общего состояния обеспечения корпоративной безопасности, пока не сформулированы единый методический подход, четкие критерии и показатели, позволяющие оценивать всю процедуру обеспечения корпоративной безопасности, ее конечные результаты и эффективность деятельности самих сотрудников подразделений безопасности.

В некоторых корпорациях в качестве оценочного критерия используется число событий и происшествий, имеющих отношение к безопасности, за текущий период. Полученные данные сопоставляются с числом событий и происшествий такого же порядка за аналогичные периоды прошлого года. Такой метод дает возможность сформировать определенное представление о некоторых сторонах обеспечения безопасности корпораций и местах их наибольшей уязвимости, но не позволяет увидеть общую картину такой деятельности, оценить все ее нюансы, выявить сильные и слабые стороны.

На данный момент распространенным и весьма успешным является также метод экспертных оценок, дающий возможность определять не только количественный, но и качественный уровень достигнутого состояния защищенности корпораций.

Развитие современных технологий обеспечения безопасности компаний раскрывает перспективы перехода от действующих сегодня нескольких разрозненных систем защиты структурных подразделений корпораций и информационных потоков к развертыванию обобщенных автоматизированных систем управления безопасностью. Внедрение в корпорациях таких систем может носить различный уровень интеграции и охвата объектов и сфер обеспечения безопасности в зависимости от организационно-правовой формы

корпораций, видов их производственной и коммерческой деятельности, а также финансовых возможностей.

Естественно, каждая компания стремится создать наиболее приемлемую для себя систему обеспечения собственной безопасности и сформировать механизм функционирования ее взаимосвязанных и взаимострахующих компонентов. Нельзя не признать, однако, что решающую роль в достижении надежной защищенности любых хозяйствующих субъектов играет все же человек, способный на должном профессиональном уровне успешно решать специфические задачи обеспечения корпоративной безопасности. Не случайно не утратило своего значения известное изречение, что кадры решают все.

Не секрет, что до настоящего времени службы безопасности корпораций комплектуются преимущественно за счет бывших сотрудников правоохранительных органов и спецслужб, обладающих необходимыми компетенциями. Недостатком такого кадрового пополнения является то, что у таких работников сложился определенный стереотип поведения, поскольку они привыкли действовать от имени всей совокупной мощи государства. К тому же далеко не все из них имеют необходимые знания в сфере рыночных отношений современной российской экономики.

По мере увеличения уязвимости бизнеса из-за нарастающего числа угроз и их усложнения все более актуальной становится проблема подготовки кадров со специализацией обеспечения корпоративной безопасности. Важный шаг для решения проблемы нехватки квалифицированных кадров был сделан, когда в начале 2017 г. в составе Международного института энергетической политики и дипломатии (МИЭП) МГИМО была создана кафедра корпоративной безопасности, основанная под эгидой ПАО «Горно-металлургическая компания «Норильский никель».

Решение о создании кафедры базировалось на анализе динамики угроз и современных тенденций в сфере обеспечения корпоративной безопасности, который показал возрастание важности этого направления деятельности корпораций и объективную потребность целенаправленного использования научных методов для повышения ее эффективности.

Кафедра корпоративной безопасности как научно-педагогическое образование специализированного профиля представляет собой пилотный проект, который, надеемся, найдет последователей в России в силу заинтересованности бизнеса в подготовке профессионалов в сфере корпоративной безопасности. В результате создается возможность использовать базу и опыт МГИМО и его институтов для изучения теории и практики обеспечения безопасности компаний за рубежом и в нашей стране с целью распространения обобщенных знаний в заинтересованных кругах российского бизнеса. Кроме того, это позволит лучшим специалистам «Норильского никеля» в ходе учебных занятий в вузе делиться со студентами своими компетенциями и практическими навыками, приобретенными компанией в процессе решения проблем обеспечения собственной безопасности. Одновременно создается устойчивая площадка для развития в этой области научно-практического диалога между государством и гражданским обществом, с одной стороны, и бизнесом с – другой.

К числу главных задач кафедры, помимо учебно-педагогической, относятся организация научных исследований всего комплекса проблем обеспечения корпоративной безопасности, сбор и систематизация данных о новейших подходах в этой области, изучение и распространение передовых стандартов и технологий, внедренных лидерами мировой и отечественной экономики в практику обеспечения безопасности компаний.

Надеемся, что в ближайшем будущем профессорско-преподавательский состав кафедры подготовит качественную учебно-методическую литературу и научные труды в относительно молодой области знаний – корпоративной безопасности, которые нуждаются в серьезном наращивании.

И последнее, что хотелось бы отметить. Деятельность по обеспечению корпоративной безопасности является непроизводственной сферой, которая не предназначена для зарабатывания денег и принесения дохода. Свою весьма высокую затратность такая деятельность компенсирует способностью сохранять и приумножать материальные и финансовые средства корпораций при грамотной ее организации через снижение рисков путем повышения производительности и эффективности бизнес-процессов.

Предлагаемые теоретические размышления фрагментарны, не затрагивают многих важных деталей и особенностей в силу ограниченного объема научной статьи как вида издания и поэтому не могут претендовать на полноту, законченность и, тем более, идеальность. Их следует рассматривать лишь как попытку внести отдельные уточнения в некоторые аспекты обеспечения корпоративной безопасности. Главная цель изложеного материала – стимулировать дискуссию, результаты которой, возможно, приведут к устранению рассогласованности в понимании упомянутых терминов, совершенствованию понятийного аппарата и системы обеспечения корпоративной безопасности в целом.

GASUMYANOV Vladislav Ivanovich, *Dr.Sci. (Econ.), Vice-President of PJSC «MMC Norilsk Nickel», Head of the Chair of Corporate Security, International Institute of Energy Policy and Diplomacy, Moscow State Institute of International Relations, University of the Ministry for Foreign Affairs of Russia (76 Vernadskogo Ave, Moscow, Russia, 119454)*

CORPORATE SECURITY IN THE NATIONAL SECURITY SYSTEM OF THE RUSSIAN FEDERATION: THEORETICAL ASPECTS

Abstract. *The article is devoted to some aspects of the developing subject area, namely the provision of corporate security as an integral part of the science of national security. The author contemplates main categories of corporate security, offers the definition of a number of its concepts, sets out his vision of the content of the corporate security system, and suggests the ways to improve it.*

Keywords: *security, national security, economic security, strategic national priorities, corporate security, challenges, risks, threats, monitoring, evaluation of corporate security findings*