руководители, не обладают четким пониманием всех факторов, обуславливающих стратегическое управление информационной безопасностью в правоохранительной сфере.

Указанное определяет необходимость развития национальной школы стратегического управления в правоохранительной сфере, выделения в ней отдельного вектора – стратегического управления информационной безопасностью, осознания и понимания уровня его развития, определения необходимости корректировки направления развития правоохранительной стратегии в будущем.

На сегодняшний день теория стратегического управления как направление в науке и практике базируется на значительном арсенале научных разработок и концепций: теории научной организации труда и социологии управления, теории социальных явлений, общей теории систем, кибернетике, концепции стратегического моделирования и планирования, современной философии менеджмента, теории управленческих решений, теории формирования стратегии как коллективного процесса, научном управлении обществом и т. д.

Современные теоретики и практики главной составляющей стратегического управления считают стратегию, улучшение технологии принятия решений и их выполнение. Проблемой стратегического управления является его развитие в качестве самостоятельного практического направления в сфере информации, а также построение теоретической концепции в рамках научной отрасли социологии управления. В настоящее время существует лишь приблизительная рабочая модель, вокруг которой необходимо построить теоретическую конструкцию. Как предметная сфера человеческой деятельности, стратегическое управление информационной безопасностью в правоохранительной сфере представляет собой подсистему социального управления, призванную обеспечить информационную безопасность личности, общества, государства в различных сферах жизнедеятельности.

Научным сообществом исследованию стратегического управления в последние годы стало уделяться значительно больше внимания. Научная деятельность в этом направлении активизировалась, прежде всего, по причине необходимости разработки теоретических основ, вызванной цивилизационными процессами в обществе и трудностями создания эффективной правоохранительной организации, которая призвана обеспечить безопасность в информационной сфере.

Увеличение числа работ, посвященных отдельным проблемным аспектам организации и реализации стратегического управления в правоохранительной сфере, связано с осознанием практиками и теоретиками необходимости полноценного формирования данного института с учетом постоянно меняющихся вызовов и угроз общественной безопасности, противодействия закону и праву, угрожающим общественным и государственным ценностям.

Безусловно, общетеоретическая значимость работ, раскрывающих теоретические основы стратегического управления, высока. Однако следует иметь в виду необходимость комплексного изучения проблемных вопросов стратегического управления информационной безопасностью в правоохранительной системе, с учетом норм времени и происходящих событий в современном мире, чтобы полученные теоретико-правовые выводы учитывали и проблемы современности, и специфику правовой системы Республики Беларусь, а потому были применимы к ней. Необходимо понимать, что в процессе движения нашего общества решающее значение приобретает выработка научно-обоснованной стратегии осуществления глубинных социально-экономических преобразований.

Исходя из изложенного, представляется необходимым стратегическое управление информационной безопасностью в правоохранительной сфере рассматривать в качестве уникальной системы, которая должна своевременно распознавать проблемы, выдвигать научно-обоснованные стратегические цели, пути и способы их достижения; формировать представления о состоянии системы в будущем с сохранением традиционных и приобретением (созданием) новых способностей и возможностей управления, подстраивающихся под изменяющиеся и открывающиеся возможности; своевременно улавливать и распознавать возможности и угрозы, исходящие из внешней среды; вырабатывать способы изменения внешнего окружения, реформирования правоохранительной сферы, системы оперативного управления по мере увеличения собственного потенциала, выполнения стратегических задач.

УДК 342.951

А.В. Калиберов

ОСОБЕННОСТИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ТАМОЖЕННЫХ ОРГАНОВ

В Послании Президента Республики Беларусь белорусскому народу и Национальному собранию в качестве одной из точек роста экономики названо повсеместное внедрение новых информационных технологий.

В системе таможенных органов функционируют 40 информационных систем и 30 баз данных по таким ключевым направлениям деятельности, как таможенный транзит, декларирование товаров и транспортных средств юридическими и физическими лицами, анализ поступления таможенных платежей, автоматизация финансово-хозяйственной деятель-

ности таможенных органов и т. д. При этом все информационные системы объединены в единую автоматизированную информационную систему таможенных органов.

Как показывает практика, применение информационных технологий в деятельности таможенных органов позволяет снизить временные затраты на оформление, обеспечить оперативность контроля, тем самым улучшить транзитную привлекательность страны.

Вместе с тем нельзя оставлять без внимания факт, что процесс информатизации таможенной сферы имеет и оборотную сторону – наряду с положительными изменениями возможны и негативные последствия, такие как использование возможностей информационных технологий в противоправных целях. Это ставит вопрос об обеспечении перехода информационной безопасности на новый уровень, тем более, с 1 января 2018 г. вступил в силу новый Таможенный кодекс Евразийского экономического союза (ТмК ЕАЭС), знаменующий собой более высокий этап не только экономической, но и информационной интеграции.

Основными причинами, которые поднимают актуальность вопросов обеспечения информационной безопасности на единой таможенной территории Евразийского экономического союза (ЕАЭС), являются:

объединение в единое информационное пространство деятельности таможенных органов государств – членов ЕАЭС, включая сопряжение их информационных систем;

динамичное развитие информационных технологий в таможенном деле, которые требуют новых адаптированных к ним подходов по обеспечению безопасности информации;

закрытость технологий и средств защиты конфиденциальной информации таможенных органов, в том числе национальной государственной тайны.

Анализ существующих подходов государств – членов ЕАЭС в решении задач по обеспечению безопасности информации показал, что они имеют в целом одни и те же взгляды на эту сферу деятельности. Так, в ТмК ЕАЭС содержится ряд норм, в которых отражены положения по регулированию деятельности таможенных органов в сфере обеспечения безопасности информации, в частности этим вопросам посвящены гл. 48 и 49.

Следует отметить, что ТмК ЕАЭС в вопросах обеспечения информационной безопасности сохранил те же подходы, которые в свое время были закреплены в действующем Таможенном кодексе Таможенного союза. Это касается, прежде всего, основополагающих положений обеспечения таможенными органами информационной безопасности:

целевое назначение получаемой таможенными органами информации (любая информация, полученная таможенными органами, используется таможенными органами исключительно для выполнения возложенных на них задач и функций);

запрет на разглашение, использование в личных целях либо передачу иным лицам получаемой таможенными органами информации;

законодательно закрепленный порядок обмена информацией между таможенными органами.

Однако надо иметь в виду, что при реализации указанных положений необходимо решить ряд вопросов, среди которых можно выделить такие, как:

1) соблюдение конституционных прав и свобод граждан в области получения и использования таможенной информации;

2) информационное обеспечение деятельности ЕАЭС, связанное с доведением до населения государств – членов ЕАЭС и международной общественности достоверной информации о его деятельности, его официальной позиции по значимым вопросам в таможенной сфере, с возможностью доступа граждан к его открытым информационным ресурсам;

3) применение и развитие современных информационных технологий собственного производства;

4) защита информационных ресурсов и информационно-телекоммуникационных технологий от угроз в сфере информационной безопасности.

Это, в свою очередь, подразумевает дальнейшее совершенствование и проведения единой политики в области обеспечения безопасности таможенных органов в условиях ЕАЭС, разработки практических мер по воплощению политики безопасности информации и выработки комплекса согласованных мер нормативно-правового, технологического и организационно-технического характера, направленных на выявление, отражение и ликвидацию последствий реализации различных видов угроз безопасности информации.

УДК 004.315.5

С.Н. Касанин

НАУЧНО-МЕТОДОЛОГИЧЕСКИЕ АСПЕКТЫ В ОБЛАСТИ ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

В Указе Президента Республики Беларусь от 9 ноября 2010 г. № 575 «Об утверждении Концепции национальной безопасности Республики Беларусь» выделены концептуальные источники угроз национальной безопасности в информационной сфере, на решение которых и направлены наши усилия.