В целях организации защиты от информационных угроз важных для государства информационных систем в Республике Беларусь создан институт критически важных объектов информатизации (КВОИ). Основополагающими документами в данной сфере являются Концепция национальной безопасности Республики Беларусь и Указ Президента Республики Беларусь от 25 октября 2011 г. № 486 «О некоторых мерах по обеспечению безопасности критически важных объектов информатизации» (далее – Указ № 486).

В соответствии с Концепцией национальной безопасности Республики Беларусь одним из основных национальных интересов в информационной сфере является обеспечение надежности и устойчивости функционирования критически важных объектов информатизации.

Указом № 486 утверждено Положение об отнесении объектов информатизации к критически важным и обеспечении безопасности критически важных объектов информатизации.

В развитие Указа № 486 утверждены следующие документы:

постановление Совета Министров Республики Беларусь от 30 марта 2012 г. № 293 «О некоторых вопросах безопасной эксплуатации и надежного функционирования критически важных объектов информатизации»;

Положение о Государственном реестре критически важных объектов информатизации приказом Оперативно-аналитического центра при Президенте Республики Беларусь (далее – ОАЦ) от 20 декабря 2011 г. № 96;

Инструкция о порядке проведения внешнего контроля за обеспечением безопасности критически важных объектов информатизации приказом ОАЦ от 30 апреля 2012 г. № 42;

Технический кодекс установившейся практики ТКП 483-2013 «Информационные технологии и безопасность. Безопасная эксплуатация и надежное функционирование критически важных объектов информатизации. Общие требования» приказом ОАЦ от 17 июля 2013 г. № 47.

Вместе с тем необходимо отметить, что, так как имеющиеся показатели уровня ущерба, в соответствии с которыми объекты информатизации относятся к КВОИ, являются неоднозначными, владельцы КВОИ испытывают затруднения при создании системы безопасности (в соответствии с требованиями системы менеджмента информационной безопасности СТБ ISO/IEC 27001), было принято решение о необходимости внесения соответствующих изменений в Указ № 486 и нормативные правовые акты, изданные в его развитие. Завершение мероприятий по внесению изменений запланировано на 2017–2018 гг.

УДК 34.09

М.В. Губич

СТРАТЕГИЧЕСКОЕ УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ В ПРАВООХРАНИТЕЛЬНОЙ СФЕРЕ

Проблемы стратегического управления в сфере безопасности в последние годы становятся все более актуальными. Это совсем не случайно, поскольку XXI в. в целом характеризуется переходом мировой цивилизации из информационной стадии в стадию интеллектуального развития. Время случайных шагов в управлении проходит, наступает время системной работы, которая становится все более сложной и интеллектуально наполненной. В связи с этим в управлении происходит естественное смещение внимания с информационных потоков на процессы принятия стратегических решений, т. е. в ту сферу, где рождаются новые знания.

На сегодняшний день стратегия информационной безопасности становится неотъемлемым компонентом любого сложного действия либо проблемной ситуации, в которой задействовано много социальных субъектов. При этом стратегия информационной безопасности является компонентом стратегии более высокого уровня – безопасности в целом. В этой связи управление процессами в информационной сфере нельзя рассматривать в отрыве от общих вопросов безопасности.

Несмотря на принимаемые в нашей стране меры, направленные на реализацию политики стратегического управления в правоохранительной сфере, – разработку и реализацию Концепции национальной безопасности Республики Беларусь, Национальной стратегии устойчивого развития и ряда иных управленческих решений, в том числе связанных с реорганизацией правоохранительной системы, – до настоящего времени она не приобрела окончательных очертаний. Представляется, что в определенной мере это связано со сложностью понимания тонкостей и нюансов данного процесса и недостаточной разработанностью алгоритма применения его в практической деятельности.

В первую очередь необходимо констатировать факт того, что стратегическое управление – самая сложная разновидность управленческой деятельности, представляющая собой совокупность множества приемов, способов и методов управления, понятийных категорий, необходимых для знания и понимания, а также включающая в себя стратегический анализ, прогнозирование и планирование. Кроме того, отдельные должностные лица правоохранительных органов, в том числе

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-