пример, конкретизировано содержание понятия «угроза безопасности государства», включающее основания для отказа в допуске к сведениям, составляющим государственную тайну. Такими основаниями будут являться:

попытка своими действиями, призывами осуществить изменение конституционного строя государства, нелегитимным путем изменить состав высших органов государственной власти; либо финансирование этой деятельности, а равно содействие данной деятельности в иной форме;

непосредственное участие в экстремистской деятельности, проявление социальной, расовой, национальной, религиозной нетерпимости в виде пропаганды превосходства по таким основаниям;

подтвержденные контакты с участниками террористических организаций и организованных преступных группировок;

попадание гражданина или его близких родственников в материальную зависимость от иностранных государств, иностранных организаций, отдельных граждан иностранных государств, в отношении которых имеются подтвержденные сведения, что они занимаются или содействуют разведывательной, а также иной противоправной деятельности.

В обсуждаемом законопроекте подробнее в сравнении с большинством национальных законодательств определены вопросы доступа должностного лица или гражданина к сведениям, составляющим государственную тайну.

Ответственность за обеспечение защиты государственной тайны на предприятиях, в учреждениях и организациях возлагается на их руководителей. Условия по защите сведений, составляющих государственную тайну, должны создаваться в органах государственной власти, на предприятиях, в учреждениях и организациях до получения (начала разработки) ими таких сведений. Законопроектом предусматривается государственная аттестация руководителей, ответственных за защиту сведений, составляющих государственную тайну. Состояние защиты государственной тайны в подведомственных организациях учитывается при проведении государственной аттестации их руководителей.

Отдельная статья законопроекта определяет вопросы защиты государственной тайны иностранных государств, секретов международных организаций, межгосударственных образований.

За нарушение законодательства о государственной тайне предусмотрена уголовная, административная, гражданско-правовая или дисциплинарная ответственность в соответствии с нормами действующего национального законодательства. При этом законопроект предусматривает, что вред, причиненный в результате нарушения законодательства о государственной тайне, подлежит возмещению в порядке, установленном актами национального законодательства.

УДК 004

Д.Н. Вяткин

НОРМАТИВНО-ПРАВОВЫЕ АСПЕКТЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КРИТИЧЕСКИ ВАЖНЫХ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ

В настоящее время, по оценке Международного союза электросвязи, Республика Беларусь по итоговому индексу развития информационно-коммуникационных технологий (ИКТ) поднялась с 52-го места в 2011 г. на 31-е в 2016 г. среди 175 стран. За данный период в Беларуси создан базовый комплекс электронного правительства, в который входят такие компоненты, как общегосударственная автоматизированная информационная система, система межведомственного электронного документооборота, государственная система управления открытыми ключами проверки электронной цифровой подписи, единое расчетное информационное пространство. Завершено строительство Республиканского центра обработки данных. Осуществляется информатизация здравоохранения, образования, социально-трудовой сферы. Основной задачей внедрения ИКТ в реальный сектор экономики является повышение эффективности управления полным циклом производства, создание интегрированных информационных систем, осуществляющих управление ресурсами предприятия.

Развитие информатизации в Республике Беларусь может привести к появлению новых угроз национальной безопасности в информационной сфере, с которыми уже столкнулись некоторые страны.

Примерами таких угроз являются следующие:

компьютерная атака, совершенная на металлургическое предприятие в Германии. Злоумышленникам удалось удаленно вывести из строя доменную печь, заразив вредоносным программным обеспечением офисную сеть, что привело к поломке оборудования и простою производства;

компьютерная атака на энергетическую систему «Прикарпатьеоблэнерго», специализирующуюся на передаче и снабжении электроэнергией потребителей в Западной Украине. Злоумышленникам удалось получить несанкционированный доступ к системе управления компании, в результате чего на протяжении нескольких часов в ряде городов отсутствовало энергоснабжение.

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