хозяйстве, которая выражается в производстве никому не нужной продукции и дефиците того, что необходимо. Огосударствление экономики порождает отсутствие экономической ответственности субъектов хозяйствования. Результаты деятельности для них не имеют особого значения, поскольку государство забирает прибыль у рентабельных предприятий, а убыточным предоставляет необходимое финансирование. По этой причине ни одно предприятие не может обанкротиться.

В то же время господствующее положение государства в экономике дает ему возможность очень быстро и беспрепятственно сконцентрировать все необходимые ресурсы для решения отдельных крупных проблем: ведения гигантских промышленных строек, реализации атомных проектов и т. д.

В связи с этим, говоря о роли государства в условиях перехода общества к рыночным отношениям, важно определить пределы государственно-правового вмешательства в экономику. Юридические нормы должны определить цели, задачи, принципы рыночных отношений, законодательным путем зафиксировать рамки и пределы вмешательства государства в экономику. По сути, речь идет о выборе способа управления экономикой. В данном случае не годится командный, административный способ, характеризующийся тотальным государственно-правовым регулированием экономики. При нем закон регламентирует все процессы производства, распределения, обмена и потребления материальных благ. Объективные закономерности развития экономики игнорируются. На наш взгляд, не подходит и второй способ, основанный на стихийном саморегулировании экономики, когда правовой и государственный механизмы самоустраняются от всякого вмешательства в хозяйственную сферу. Наиболее приемлемым представляется третий, смешанный способ, сочетающий рыночные законы с разумным правовым регулированием экономики, рынка сбыта, рабочей силы и т. д. Этот способ государственно-правового управления экономикой содействует ее поступательному развитию, поскольку государство защищает свободное предпринимательство от кризисов, предпринимает меры по предотвращению спада производства, кризиса хозяйственной жизни, используя при этом юридические формы таких экономических рычагов, как налоги, кредиты, инвестиции и др.

Исходя из вышеизложенного, можно обозначить основные направления деятельности государства в условиях перехода общества к рыночным отношениям. Они заключаются в том, что государство должно стать:

гарантом правовых рамок хозяйственной жизни, правовых отношений всех субъектов производства и обращения;

непосредственным владельцем и управленцем строго ограниченного сектора экономики;

совладельцем, пайщиком предприятий со смешанной формой собственности и не только в сфере материального производства, но и в других областях, например средств массовой информации;

фискальным институтом, т. е. сборщиком налогов, контролером всех участников хозяйственного оборота (но исключительно на экономической и правовой основе), собственником национальной казны и эмиссионного центра;

главным (но не единственным) инвестором общенациональных экономических, экологических, научных и других программ;

гарантом соблюдения общегосударственных экономических, научно-технических интересов страны в международных отношениях;

инструментом гармонизации через планирование, программирование, посредничество и т. д. экономических и социальных интересов, потребностей как различных регионов, так и социальных групп, а также инструментом разрешения конфликтов.

УДК 657.6:004(045)

С.Ю. Воробьёв

ПРОВЕДЕНИЕ ИТ-АУДИТА ДЛЯ ПОВЫШЕНИЯ УСТОЙЧИВОСТИ ФУНКЦИОНИРОВАНИЯ КРИТИЧЕСКИ ВАЖНЫХ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ В СФЕРЕ ЭКОНОМИКИ

XXI в. ознаменовался появлением такого нового вида вооруженных конфликтов, как гибридная война. Одним из элементов гибридной войны являются кибератаки – целенаправленные воздействия программных и (или) программно-аппаратных средств на объекты информационной инфраструктуры, сети электросвязи, используемые для организации взаимодействия таких объектов, в целях нарушения и (или) прекращения их функционирования и (или) создания угрозы безопасности обрабатываемой такими объектами информации.

В США функционирует концепция дешевой войны (War on the Cheap), апологеты которой утверждают, что 1 млн долларов и 20 человек, осуществляя компьютерные атаки в цифровой среде, могут обеспечить успех, сопоставимый с действиями крупной армии (при этом считается, что относительно небольшими силами и средствами при минимальных финансовых затратах можно вывести из строя военную

и государственную информационную инфраструктуру противника, так что на ее восстановление потребуются годы).

Так, США в 2009 г. при помощи программы-червя Stuxnet провели серию секретных кибератак на иранские атомные объекты. Задача червя заключалась в том, чтобы заставить роторы центрифуг на атомном заводе в Нетензе раскрутиться до опасно высокой скорости вращения. Разрушение значительного количества центрифуг на объекте в Нетензе в период с 2009 по 2010 г. большинство исследователей связывают с вредоносными последствиями воздействия Stuxnet (по заявлению США, это позволило отбросить иранскую военную ядерную программу на два года назад). Необходимо отметить, что доказательства существования данной вредоносной программы были обнаружены в июне 2010 г. белорусской антивирусной компанией.

Члены НАТО признают, что кибератаки могут быть столь же опасны, как и вооруженные атаки, поэтому киберзащита признается неотъемлимой частью основной задачи НАТО – коллективной обороны. Известный киберполигон НАТО в Эстонии сегодня является базой для многочисленных учений и тренировок. Он работает формально под управлением Сил обороны Эстонии. Киберполигон обеспечивает проведение флагманских учений НАТО по киберзащите «Кибер Коалиция», которые проходят на ежегодной основе.

Глава государства на тематических совещаниях и встречах неоднократно поднимал вопросы кибербезопасности, а также отмечал, что кибератаки являются одним из опаснейших элементов гибридной войны, при котором воздействию подвергаются прежде всего стратегические объекты, государственные органы, предприятия, банковская система, т. е. основные пункты жизнеобеспечения любого государства, а целью противника является нанесение максимального ущерба экономике и дестабилизация общества.

Киберпространство – весьма специфическая сфера деятельности, среда, которая имеет относительно автономный характер и оказывает огромное влияние на развитие экономики, политической жизни, культуры, техносферы, военного дела. Задача повышенной сложности в этой сфере – выявление источника угрозы и кибератак, устранение эффекта анонимности.

Ряд отраслей национальной экономики «завязаны» на кибербезопасности, в связи с этим важно обеспечить надлежащую и эффективную защиту промышленности, энергетики, реального сектора экономики, государственных органов и учреждений, а также различных организаций (так, попадание некоторой стратегически важной информации на

серверы, контролируемые США и НАТО, принесет огромный ущерб национальной безопасности государства).

Банковская система является составной частью финансово-кредитной системы Республики Беларусь. Согласно Концепции национальной безопасности Республики Беларусь, утвержденной Указом Президента Республики Беларусь от 9 ноября 2010 г. № 575, национальными интересами являются: в экономической сфере – сохранение устойчивости финансовой и денежно-кредитной систем, в информационной сфере – обеспечение надежности и устойчивости критически важных объектов информатизации. Необходимо сфокусировать внимание как на применении банками новейших достижений ИТ-отрасли, что, в свою очередь, вызывет рост предоставления цифровых услуг, в том числе дистанционного банковского обслуживания, при которых необходимость нахождения клиента непосредственно в кредитно-финансовом учреждении отсутствует, так и на широком внедрении в Республике Беларусь безналичных расчетов с использованием банковских платежных карточек и развитии инфраструктуры обслуживания держателей таких карточек.

Услуги по операциям с участием банковских платежных карточек, в том числе авторизацию карточных операций, ведение идентификационных баз данных карточек, банкоматов и терминалов, персонализацию карточек, процессинг и клиринг операций с карточками платежных систем, подключение и обслуживание банкоматов и терминалов в точках продаж, осуществляют процессинговые центры. Согласно подп. 1.31 п. 1 ст. 2 Закона Республики Беларусь от 19 апреля 2022 г. № 164-З «О платежных системах и платежных услугах» под процессингом понимают деятельность по сбору и обработке информации, содержащейся в платежных указаниях (платежных инструкциях), и передаче обработанной информации для проведения расчетных операций.

Согласно п. 5 Положения о порядке отнесения объектов информатизации к критически важным объектам информатизации, утвержденного Указом Президента Республики Беларусь от 16 апреля 2013 г. № 196 «О некоторых мерах по совершенствованию защиты информации», одним из критериев отнесения объектов информатизации к критически важным является критерий экономической значимости, применяющийся в отношении объектов информатизации, обеспечивающих функционирование объектов (организаций) основных отраслей экономики и (или) иные важные экономические потребности, в том числе обеспечивающих проведение безналичных (межбанковских) расчетов, осуществляющих процессинг.

Для получения достоверной и систематизированной информации с целью оценки состояния информационной структуры вышеуказанных учреждений, принятия взвешенных и адекватных управленческих ре-

шений осуществляется аудит информационных технологий (далее – ИТ-аудит).

ИТ-аудит решает комплексную задачу получения актуальной и достоверной информации о текущем уровне качества функционирования информационных (-ой) систем (-ы) в организации.

Банки и небанковские кредитно-финансовые организации, а также процессинговые центры проводят аудиты на соответствие требованиям стандартов, которые не являются обязательными для применения на территории Республики Беларусь, однако применяются последними при выполнении бизнес-процессов и осуществлении производственной деятельности, например: ИСО 27001 (международный стандарт по информационной безопасности), PCI DSS (стандарт безопасности данных индустрии платежных карт), программа безопасности пользователей SWIFT.

Положением о порядке технической и криптографической защиты информации, обрабатываемой на критически важных объектах информатизации, утвержденным приказом Оперативно-аналитического центра при Президенте Республики Беларусь от 20 февраля 2020 г. № 66 «О мерах по реализации Указа Президента Республики Беларусь от 9 декабря 2019 г. № 449», закреплен обязательный ежегодный аудит системы информационной безопасности критически важного объекта информатизации.

Государственным стандартом СТБ 34.101.42–2013, а также техническими требованиями и правилами Национального банка Республики Беларусь ТТП ИБ 2.1–2020 устанавливаются требования к проведению аудита информационной безопасности банков банковской системы Республики Беларусь. Вместе с тем в соответствии с Концепцией обеспечения кибербезопасности в банковской сфере, утвержденной постановлением Правления Национального банка Республики Беларусь от 20 ноября 2019 г. № 466, вышеуказанные технические нормативные правовые акты носят рекомендательный характер и не являются обязательными к исполнению банками, Национальным банком Республики Беларусь. Для придания названным актам статуса технических нормативных правовых актов, обязательных для соблюдения всеми субъектами банковской сферы, потребуется внесение изменений в Банковский кодекс Республики Беларусь.

Постановлением Совета Безопасности Республики Беларусь от 18 марта 2019 г. № 1 «О Концепции информационной безопасности Республики Беларусь» нормативно закреплена заинтересованность государства во взаимодействии с ИТ-компаниями, интернет-провайдерами, операторами связи и внешними экспертами в обновлении и развитии

механизмов выявления угроз информационной безопасности через ИТ-аудит, мониторинг киберрисков, поиск уязвимостей и актуальных средств защиты, выработку правил поведения в сети Интернет.

Республика Беларусь находится в сложных окружающих условиях, в том числе в экономической и информационной сферах, с продолжающимися попытками кибератак на критически важные объекты экономики. Для оценки функционирования информационных систем банковской сферы, процессинговых центров, иных критически важных объектов информатизации в сфере экономики, эффективности влияния последних на основные бизнес-процессы необходимо проведение аудита (-ов) информационных технологий. Осуществление аудитов информационной безопасности закреплено как в национальном законодательстве, так и в международных стандартах и носит, как правило, рекомендательный характер. Вместе с тем проведение обязательного для субъектов банковской сферы ИТ-аудита требует внесения изменений и дополнений в действующие нормативные правовые и технические нормативные правовые акты.

УДК 34.07

В.С. Гальцов

ВОПРОСЫ ПРАВООХРАНИТЕЛЬНОЙ ПОЛИТИКИ В ОБЛАСТИ РАЗВИТИЯ СОДЕРЖАНИЯ СТАТУСА ГОСУДАРСТВЕННЫХ ОРГАНОВ КАК СУБЪЕКТОВ СИСТЕМЫ ОБЕСПЕЧЕНИЯ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ

В настоящее время развитие белорусской государственности характеризуется плановыми общественными, экономическими, военно-политическими и иными преобразованиями, отличающимися высокой интенсивностью и динамичностью. Следует констатировать при этом, что жизнедеятельность белорусского государства, общества и отдельного человека затронуты геополитическими и внутренними процессами, которые генерируют задачи по укреплению национальной безопасности. Так, отдельными силами предпринимаются попытки путем введения санкций, применения методов гибридной войны, дестабилизации различных сфер жизни нарушить сложившийся баланс интересов личности, общества и государства, сформировать и навязать чуждую белорусам идеологию, призванную подменить или исказить традиционные духовно-нравственные ценности народов, населяющих Республику Беларусь. В связи с этим в складывающейся ситуации одной из важней-