мается состояние, достигаемое применением организационных, правовых и технических мер по защите информации, а также систематическим повышением уровня подготовки специалистов, реализующих названные меры. Изменение каждого из этих элементов неизбежно оказывает влияние на остальные. Так, стремительное развитие сферы информационно-коммуникационных технологий требует своевременного редактирования отдельных нормативных правовых актов и технических правовых актов. Учитывая указанное обстоятельство, ОАЦ осуществляет систематическую работу по совершенствованию законодательства в сфере защиты информации.

В ближайшее время развитие названной отрасли законодательства будет определяться тремя основными факторами.

Во-первых, подготовкой и принятием Закона Республики Беларусь «О персональных данных», который позволит однозначно определить понятийный аппарат, категории персональных данных, принципы работы и основы правового регулирования порядка обработки и защиты персональных данных, права субъектов персональных данных и обязанности операторов при их обработке, порядок трансграничной передачи персональных данных, а также установить контроль и ответственность в сфере работы с персональными данными.

Вторым фактором будет выступать принятие новой редакции стандарта Республики Беларусь 34.101.30 «Информационные технологии. Методы и средства безопасности. Объекты информатизации. Классификация». В основе новой классификации объектов информатизации лежат такие признаки, как вид информации в зависимости от категории доступа, наличие подключения к открытым каналам передачи данных, а также конкретный тип информации, распространение и (или) предоставление которой ограничено. Избранный подход формирует множество классов, что позволяет предъявлять более дифференцированные требования по защите информации существующих и перспективных информационных систем.

Третьим фактором является разработка серии стандартов на специализированные средства защиты информации (DLP, SIEM, IPS/IDS), принятие которых позволит существенно снизить стоимость и время прохождения процедуры подтверждения соответствия требованиям технического регламента Республики Беларусь «Информационные технологии. Средства защиты информации. Информационная безопасность» (ТР2013/027/BY), так как исключит необходимость разработки и оценки заданий по безопасности.

УДК 342.951; 351.9; 34:002

Д.В. Перевалов

ПРОБЛЕМНЫЕ ВОПРОСЫ ФУНКЦИОНИРОВАНИЯ СПЕЦИАЛЬНОГО КОМПЛЕКСНОГО АДМИНИСТРАТИВНО-ПРАВОВОГО РЕЖИМА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ КРИТИЧЕСКИ ВАЖНЫХ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ

Должное обеспечение безопасности критически важных объектов информатизации (КВОИ) в современных условиях может быть реализовано только в рамках соответствующего специального комплексного административно-правового режима (СКАПР). Формирование такого административно-правового режима обусловлено следующими обстоятельствами.

Во-первых, СКАПР позволяет построить эффективную охрану и защиту соответствующих объектов от различного рода угроз. Во-вторых, он обеспечивает необходимый уровень охраны и защиты соответствующих объектов, что возможно только при наличии должного государственно-управленческого воздействия: общественные отношения, возникающие, изменяющиеся и прекращающиеся в процессе обеспечения безопасности КВОИ, носят преимущественно административно-правовой характер. В-третьих, СКАПР обеспечивает безопасности КВОИ комплексно, так как при его функционировании реализуются нормы сразу нескольких отраслей права – конституционного, международного, административного, уголовного, трудового, а также права технического регулирования; требования и правила данного режима затрагивают различные по характеру права и обязанности субъектов режимного регулирования.

Вместе с тем для СКАПР при обеспечении безопасности КВОИ определяющими являются нормы административного права, поскольку складывающиеся отношения, хоть и относятся к другим правовым отраслям, но в рамках очерчиваемой СКАПР сферы облекаются в административно-правовую форму и становятся объектом административно-правового регулирования.

Однако в виде СКАПР система обеспечения безопасности КВОИ в настоящее время урегулирована нормативно не в должной степени. В то же время в связи с увеличением числа и изменением характера информационных угроз, возрастанием значения КВОИ в жизнедеятельности государства и общества все более актуальной становится потребность в более широком правовом регулировании данной сферы.

Исходя из сложившихся подходов к сущности и содержанию административно-правовых режимов и основываясь на результатах прове-

денных исследований, можно определить, что содержание СКАПР при обеспечении безопасности КВОИ должны составлять следующие элементы.

1. Нормативно-правовая основа СКАПР при обеспечении безопасности КВОИ.

Нормативно-правовую основу рассматриваемого СКАПР составляет совокупность следующих групп правовых норм:

1) нормы специального законодательного акта в области обеспечения безопасности КВОИ, которые определяют правовой статус КВОИ; субъектов государственного управления в этой сфере и их функции; систему и содержание мер обеспечения безопасности КВОИ, порядок их применения и др.;

2) нормы законодательных актов, постановлений Правительства Республики Беларусь, а также предписания нормативных правовых актов уполномоченных государственных органов и собственников (владельцев) КВОИ, детализирующие вопросы реализации мер обеспечения безопасности КВОИ;

3) нормы актов законодательства, непосредственно не регламентирующие обеспечение безопасности КВОИ, но создающие условия по реализации мер обеспечения их безопасности, а также определяющие полномочия государственных органов и иных организаций по реализации таких мер.

В настоящее время вопросы обеспечения безопасности КВОИ регламентируются Указом Президента Республики Беларусь от 25 октября 2011 г. № 486 «О некоторых мерах по обеспечению безопасности критически важных объектов информатизации» (далее – Указ № 486), постановлением Совета Министров Республики Беларусь от 30 марта 2012 г. № 293 «О некоторых вопросах безопасной эксплуатации и надежного функционирования критически важных объектов информатизации», а также приказами Оперативно-аналитического центра при Президенте Республики Беларусь (ОАЦ) и техническими нормативными правовыми актами.

Вместе с тем при осуществлении правового регулирования обеспечения безопасности КВОИ возникает ряд проблем, основной из которых является сопряжение технических аспектов обеспечения безопасности КВОИ и закономерностей правовой регламентации данной сферы общественных отношений.

Наличие данной проблемы обусловлено следующими обстоятельствами:

1) вовлечение деятельности по обеспечению безопасности КВОИ в сферу правового регулирования имеет определенные последствия:

подчинение этой деятельности принципам правового регулирования (использование правовых дефиниций, определение правового статуса субъектов, определение вида и характера действий, установление процедурного порядка осуществления действий);

определение пределов осуществления деятельности по обеспечению безопасности КВОИ (осуществление действий только по технической защите информации или иных действий);

установление при осуществлении деятельности по обеспечению безопасности КВОИ общеобязательных и унифицированных правил поведения (невыполнение этих действий влечет административную или уголовную ответственность – например, нарушение правил защиты информации (ст. 22.7 Кодекса Республики Беларусь об административных правонарушениях) или умышленное нарушение правил эксплуатации компьютерной системы или сети (ст. 355 Уголовного кодекса Республики Беларусь);

2) деятельность по обеспечению безопасности КВОИ имеет свою специфику:

такая деятельность в большинстве своем регулируется различными техническими нормативными правовыми актами;

функционирование программно-аппаратных средств невозможно урегулировать нормативными правовыми актами.

В связи с этим требуется принятие законодательного акта (внесение изменений в Указ № 486), который бы в полном объеме регулировал отношения в сфере обеспечения безопасности КВОИ.

2. Субъекты режимной деятельности, осуществляемой в рамках СКАПР при обеспечении безопасности КВОИ.

К таким субъектам относятся ОАЦ и его уполномоченные должностные лица. Вместе с тем существует объективная потребность в расширении субъектов рассматриваемого СКАПР, в частности при осуществлении в отношении КВОИ режимной деятельности по обработке информации, содержащей государственные секреты.

3. Объекты, на которые направлена режимная деятельность, осуществляемая в рамках СКАПР при обеспечении безопасности КВОИ.

Режимная деятельность, осуществляемая в рамках рассматриваемого СКАПР, должна быть направлена:

1) на критические элементы КВОИ, т. е. его структурные компоненты, полное или частичное разрушение, выход из строя или невозможность действовать которых с неизбежностью приводят к нарушению или прекращению функционирования КВОИ в целом (аппаратные и программные средства, руководство и отдельные специалисты КВОИ и т. п.);

2) уязвимые места КВОИ – те его участки, зоны или сегменты критических элементов КВОИ, в отношении которых в силу их недостаточной устойчивости или низкого уровня защищенности могут быть успешно реализованы незаконные действия (электрокабели, провода связи, мотивация и здоровье персонала объекта и т. п.);

3) деяния, совершаемые в отношении критических элементов или уязвимых мест КВОИ, либо иные деяния, создающие угрозу безопасности КВОИ.

Адекватная и эффективная режимная деятельность должна основываться на знании и прогнозировании возможных действий лиц, создающих угрозы безопасности КВОИ, – нарушителей безопасности КВОИ.

4. Режимная деятельность уполномоченных субъектов по установлению, поддержанию и прекращению действия СКАПР при обеспечении безопасности КВОИ.

Целью осуществления режимной деятельности субъектов СКАПР при обеспечении безопасности КВОИ является охрана и защита, обеспечивающие соблюдение интересов государства и общества, а также нормальное функционирование объекта или поддержание его функционирования в случае выхода из строя его компонентов.

Установление СКАПР осуществляется принятием соответствующего законодательного акта, который регламентирует отношения в рассматриваемой области, определяет критическую информационно-коммуникационную инфраструктуру с выделением КВОИ и включением таких объектов в Государственный реестр КВОИ. Рассматриваемый СКАРП фактически установлен принятием Указа № 486. Одновременно сформирован соответствующий Государственный реестр.

Содержанием деятельности субъектов рассматриваемого СКАПР по поддержанию данного режима должна стать реализация соответствующих правовых, организационных, инженерно-технических, аппаратно-программных и специальных мер обеспечения безопасности КВОИ. Вместе с тем очевидно, что система мер обеспечения безопасности КВОИ сформирована еще не в полной мере, так как основной упор пока делается на аппаратно-программные и инженерно-технические меры.

Действия по прекращению действия СКАПР при обеспечении безопасности КВОИ будут заключаться в выводе соответствующих объектов из числа критически важных и в исключении их из Государственного реестра КВОИ.

УДК 343

Д.Г. Полещук

НЕЗАКОННЫЙ ОБОРОТ ПАРОЛЕЙ, КОДОВ ДОСТУПА К КОМПЬЮТЕРНОЙ СИСТЕМЕ, СЕТИ ИЛИ МАШИННОМУ НОСИТЕЛЮ: ПЕРСПЕКТИВЫ КРИМИНАЛИЗАЦИИ

Общество XXI в. характеризуется скоростными темпами развития информационных технологий, повышением значения информации и подавляющим воздействием глобальной компьютерной сети Интернет на повседневную жизнь большинства людей. На рабочих местах, в домашних условиях, в транспорте используются компьютеры, планшеты, смартфоны и иные устройства, позволяющие осуществлять быстрый доступ к различным информационным системам или сетям (в том числе социальным). В основном такой доступ носит санкционированный характер, то есть для его осуществления требуется идентификация пользователя путем введения его логина и пароля (кода) доступа, только пароля (кода) доступа либо использования дополнительных средств защиты от незаконного доступа (например, подтверждение доступа посредством SMS-информирования). Одновременно на многих машинных носителях (компьютеры, мобильные устройства и др.) также устанавливаются пароли (коды) доступа и даже сканеры отпечатков пальцев с целью ограничения доступа к таким устройствам посторонних лиц. Осуществление указанных технических мер обусловлено необходимостью защиты хранящейся в компьютерной системе, сети или на машинных носителях информации, ценной для их пользователей, владельцев и собственников.

Вместе с тем попытки несанкционированного доступа к защищенной информации приобрели маштабность мирового значения, а борьба с ними стала одной из ключевых проблем в сфере обеспечения информационной безопасности.

В то же время вопросам оборота паролей, кодов доступа к компьютерной системе, сети или машинному носителю (далее – пароли), полученным незаконным путем, в национальном охранительном законодательстве и в юридической литературе особого внимания не уделяется. С точки зрения действующего законодательства незаконные действия с паролями (продажа, отчуждение в иной форме, приобретение и др.) теоретически не могут рассматриваться как приготовление к преступлению (ст. 349 УК Республики Беларусь) или административному правонарушению (ст. 22.6 КоАП Республики Беларусь), поскольку КоАП не выделяет приготовление к административному правонарушению как основание наступления административной ответственно-