

Полученные же кредитополучателем денежные средства (кредит) в дальнейшем могут быть использованы им в качестве объекта инвестиций (вложения в различные инвестиционные проекты с целью получения прибыли), при этом такие действия никоим образом не влияют на исполнение обязанности перед кредитором по возврату предмета договора.

Следует отметить, что сегодня в мире в силу специфики современных экономических отношений с их непредсказуемостью и высокими рисками четко прослеживается тенденция к смещению вектора финансирования от инвестирования в сторону предоставления кредитных ресурсов их получателям. Полагаем, что в целях реализации государственных мер по обеспечению экономической безопасности Республики Беларусь инвестиционная политика государства в этой части должна быть скорректирована.

УДК 342.9

Д.В. Первалов

ОТДЕЛЬНЫЕ ОРГАНИЗАЦИОННО-ПРАВОВЫЕ ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ КРИТИЧЕСКИ ВАЖНЫХ ОБЪЕКТОВ В СОВРЕМЕННЫХ УСЛОВИЯХ

Все более актуальный характер во многих странах, в том числе в Республике Беларусь, приобретает проблема обеспечения безопасности критически важных объектов (КВО). В последние 10 лет получила развитие правовая регламентация обеспечения безопасности КВО в целом. Ряд соответствующих мер предусматриваются: Концепцией борьбы с терроризмом в Республике Беларусь, утвержденной постановлением Совета Министров Республики Беларусь от 25 июля 2013 г. № 658; Указом Президента Республики Беларусь от 17 августа 2015 г. № 356 «О комиссии по противодействию экстремизму и борьбе с терроризмом»; Законом Республики Беларусь от 3 января 2002 г. № 77-3 «О борьбе с терроризмом»; Положением о профилактических, режимных и организационных мерах предупреждения террористической деятельности и минимизации ее последствий на критически важных объектах Республики Беларусь, утвержденным постановлением Комитета государственной безопасности Республики Беларусь и Министерства внутренних дел Республики Беларусь от 30 сентября 2016 г. № 24/268. Вместе с тем имеется ряд проблем, на основные из которых целесообразно обратить внимание.

Предметом правового регулирования в сфере безопасности КВО должны являться две взаимосвязанные, но разные по своему содержанию области – обеспечение безопасного функционирования системы КВО и обеспечение безопасности КВО. Обеспечение безопасного функционирования КВО представляет собой выделение среди объектов социально-экономической инфраструктуры государства критически важных и поддержание их безопасного функционирования в соответствии с правилами и требованиями, предъявляемыми к реализуемым на них технологическим процессам, – реализация мер, связанных с определенными технологическими или социальными процессами. Обеспечение безопасности КВО – это важнейшая составная часть обеспечения национальной безопасности государства, которая представляет собой правомерную деятельность работников КВО, осуществляемую во взаимодействии с сотрудниками государственных органов (организаций) и иными лицами, по реализации системы правовых, организационных, инженерно-технических, программно-аппаратных и специальных мер, направленных на охрану и защиту КВО от внешних и внутренних угроз и обеспечивающих соблюдение интересов государства и общества. При этом обеспечение безопасности КВО не является составной частью обеспечения безопасного функционирования КВО, поскольку в этих областях разные объекты, субъекты, содержание и цели государственного управления.

Обеспечение безопасности КВО целесообразно рассматривать как систему, состоящую из трех основных компонентов. Первый компонент – противокриминальная защита, она осуществляется во взаимодействии с правоохранительными органами, предусматривает защиту от правонарушений и преступных посягательств, защищает имущество собственника, жизнь и здоровье работников объекта, обеспечивает охрану общественного порядка. Второй компонент – антитеррористическая защита, она осуществляется во взаимодействии с органами безопасности, предусматривает защиту от актов терроризма и иных террористических проявлений, защищает жизнь и здоровье людей, обеспечивает государственную безопасность. Третий компонент – обеспечение информационной безопасности, она осуществляется во взаимодействии с уполномоченными государственными органами (Оперативно-аналитический центр при Президенте Республики Беларусь), предусматривает защиту от несанкционированного доступа к информационным активам и компьютерных атак, защищает информационные ресурсы и автоматизированные системы управления, обеспечивает информационную безопасность. В этом контексте, в частности, требуется корректировка определения понятия КВО в законодательстве Республики Беларусь, так как, во-первых, имеющаяся трактовка КВО делает уклон исключительно на их антитеррористическую защиту; во-вторых, она предусматривает чрезмерно обобщенный подход к выработке критериев, не предполагающий разделение видов КВО по каким-либо существенным, определяющим признакам; в-третьих, каждый КВО рассматривается как отдельный объект, а не элемент инфраструктуры, и это приводит не только к необходимости выработки мер безопасности обособленно в каждом случае, но и к разрозненности в оценке вредных (опасных) воздействий и в выработке мер предупреждения, локализации и ликвидации последствий для конкретных отраслей.

В качестве субъектов обеспечения безопасности КВО необходимо рассматривать не только уполномоченные государственные органы, но и структурные подразделения КВО, основной функцией которых является непосредственная реализация мер обеспечения безопасности данных объектов, – службы безопасности или подразделения охраны. При этом на такие службы безопасности (подразделения охраны) возлагается основная обязанность по обеспечению безопасности КВО и предоставляется соответствующий правовой статус для этого. Вместе с тем во многих случаях администрация (собственники) КВО, несмотря на социально-экономические реалии, по-прежнему считают обеспечение безопасности таких объектов исклю-

чительной компетенцией соответствующих государственных органов. При этом они полагают, что и финансовые издержки на создание системы обеспечения безопасности КВО должно нести государство. Одновременно администрация (собственники) КВО в ряде случаев заинтересованы в сокрытии фактов инцидентов безопасности на объектах, так как предание их гласности может повлечь за собой привлечение виновных лиц из числа владельцев (собственников) КВО, его руководства и иных работников объекта к уголовной, административной или иным установленным видам ответственности, а также значительные расходы на устранение причин и условий их возникновения.

Создание и поддержание системы обеспечения безопасности КВО требуют значительных финансовых ресурсов. Например, в 2004 г. хозяйствующие субъекты транспортной деятельности в РФ на обеспечение безопасности затратили собственных средств около 1,2 млрд р. (примерно 41 млн долл. США). Уже в 2011 г. только ОАО «РЖД» на цели обеспечения транспортной безопасности выделило 12,77 млрд р. (около 425 млн долл. США). При этом специалистами отмечается, что затраты на создание и поддержание систем обеспечения транспортной безопасности необходимо соотносить с возможными рисками. Так, в результате взрыва в зале международных прилетов московского аэропорта Домодедово 24 января 2011 г. погибли 37 человек и 159 причинен различной степени тяжести вред здоровью, материальный ущерб составил 40 520 928 р. (примерно 1,35 млн долл. США). Между тем планируемые в 2014 г. затраты ОАО «Авиационная компания «Трансаэро» составили бы 22 млрд 720 млн р. (примерно 570 млн долл. США), а в государственном унитарном предприятии Москвы «Московский ордена Ленина и ордена Трудового Красного Знамени метрополитен имени В.И. Ленина» – 24,357 млрд р. (примерно 600 млн долл. США).

В настоящее время установлен целый ряд требований и правил в области обеспечения безопасности КВО. Вместе с тем не предусмотрена ответственность за неправомерное вмешательство в деятельность КВО и нарушения в области обеспечения безопасности КВО. Фактически отсутствуют организационно-правовые механизмы, обеспечивающие пресечение актов незаконного вмешательства в функционирование КВО, а также за принудительное выполнение администрацией (собственниками) КВО соответствующих требований и правил.

В целях преодоления указанных и иных проблем в сфере обеспечения безопасности КВО на современном этапе представляется целесообразным:

рассмотреть вопрос о принятии законодательного акта в сфере безопасности КВО;

внести изменения и дополнения в Уголовный кодекс Республики Беларусь и Кодекс Республики Беларусь об административных правонарушениях в части, касающейся установления соответствующих видов ответственности за неправомерное вмешательство в деятельность КВО, а также за нарушения в области обеспечения безопасности КВО;

дальнейшее развитие системы обеспечения безопасности КВО осуществлять с использованием в том числе механизмов государственно-частного партнерства.

УДК 343.3

В.И. Пикта

СОДЕРЖАНИЕ ИСПОЛЬЗОВАНИЯ ПРОГРАММ-ВЫМОГАТЕЛЕЙ КАК УСЛУГИ

В последние годы стремительно расширяется инструментарий киберпреступников, что позволяет даже тем, кто не обладает техническими знаниями, проводить атаки на информационные системы с использованием различного вредоносного программного обеспечения. Одним из новейших способов совершения киберпреступлений является использование программ-вымогателей как услуги (RaaS – Ransomware as a Service). Защита от данного вида преступления очень важна, поскольку использование программ-вымогателей как услуги может повлечь за собой значительные последствия для физических лиц и организаций. Атаки RaaS могут привести к шифрованию конфиденциальных данных и потере доступа к важным системам, что ведет к значительным сбоям в работе информационных систем и финансовым потерям.

Для организаций атака RaaS может привести к потере доходов, подрыву репутации и долгосрочным финансовым потерям. В некоторых случаях организации могут быть вынуждены заплатить выкуп, чтобы восстановить доступ к своим данным, что только сильнее побуждает организаторов к совершению еще большего количества аналогичных преступлений ввиду их высокой эффективности. Кроме того, атаки RaaS могут повлечь за собой проблемы соблюдения требований нормативных правовых актов, поскольку от организаций может потребоваться сообщить государственным органам о компрометации персональных данных.

Для физических лиц RaaS-атака может привести к потере личной информации и финансовым потерям. В некоторых случаях злоумышленники могут потребовать от жертв оплату за восстановление доступа к их личным файлам.

Программа-вымогатель как услуга (RaaS) – это преступная бизнес-модель, в которой киберпреступники предлагают свои инструменты и услуги другим лицам или группам обычно за процент от суммы выкупа. Поставщики программ-вымогателей обычно предлагают ряд услуг, включая предоставление вредоносного кода программы, хостинг веб-сайта для оплаты выкупа и поддержку клиентов, осуществляющих атаки.

Программа-вымогатель является типом вредоносных программ, которые шифруют файлы жертвы и требуют выкуп в обмен на ключ для расшифровки. Обычно данная разновидность вредоносных программ распространяется через фишинговые письма или путем использования уязвимостей в программном обеспечении.

Одной из основных проблем при выявлении и раскрытии преступлений, связанных с использованием программ-вымогателей как услуги, является идентификация лиц или групп, стоящих за такими атаками. Поставщики данной услуги часто используют анонимные способы оплаты и сложную сетевую инфраструктуру, чтобы скрыть свою личность. Кроме того,