Следовательно переход всей полноты ответственности владельца транспортного средства на иное лицо возможен в силу таких законных оснований, как передача права собственности (п. 2 ст. 210 ГК), а также заключение договора аренды транспортного средства без экипажа (ст. 613 ГК), выдачу доверенности (ст. 186 ГК), а равно издание распоряжения соответствующим органом о передаче ему источника повышенной опасности и т. п. (абзац 2 п. 1 ст. 948 ГК).

Ограничение правомочия пользования транспортным средством, в виду необходимости наличия специального права на его управление не имеет юридического значения для возложения ответственности на владельца данного транспортного средства в порядке и на условиях, предусмотренных ст. 948 ГК. В то же время исключение в гражданско-правовой сфере составляет запрет на подобное использование транспортного средства, предусмотренный в п. 2 ст. 210 ГК. Кроме того, подобные действия, выразившиеся в управлении транспортным средством, в случае отсутствия оснований на его управление влекут последствия в виде не наступления страхового случая при обязательном страховании гражданской ответственности по договору комплексного страхования (абзац 4 ч. 3 п. 125 Положения).

Таким образом, изложенное позволяет сделать вывод о том, что транспортное средство, являясь особым объектом гражданских прав (источником повышенной опасности), обладает специальным правовым режимом, предполагающим большую ответственность его владельца, что в определенной мере сказывается на снижении травматизма и гибели людей (участников дорожного движения).

УДК 342.91

Т.Г. Чудиловская

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ЭЛЕКТРОННОГО ПРАВИТЕЛЬСТВА

В настоящее время актуальна тема формирования электронного правительства и оказания государственных услуг в электронном виде. Концепция электронного правительства, появившаяся в 1990-х гг., подразумевает максимальное использование в органах государственного управления современных информационно-коммуникационных технологий, в том числе интернета. Их цель – повышение эффективности работы на различных уровнях: между государством и гражданами (G2C – Government-to-Citizen), между государством и бизнесом (G2B – Government-to-Business), между государством и государственными служащими (G2E – Government-to-Employees), между различными ветвями государственной власти (G2G – Government-to-Government).

В основе деятельности электронного правительства лежит электронное информационное взаимодействие государственных организаций и органов власти всех уровней как между собой, так и с иными физическими и юридическими лицами. Процессы развития электронных услуг остро ставят вопросы цифрового доверия. Доверие граждан и предприятий к государственным услугам, предоставляемым в электронном виде, напрямую зависит от уровня обеспечения информационной безопасности инфраструктуры электронного правительства и взаимодействующих элементов.

В процессе получения государственных услуг субъекты информационных отношений заинтересованы в обеспечении:

конфиденциальности (сохранения в тайне) определенной части информации;

достоверности, актуальности, целостности информации;

защиты от навязывания им ложной (недостоверной, искаженной) информации;

возможности осуществления непрерывного контроля и управления процессами обработки и передачи информации;

защиты части информации от незаконного ее тиражирования;

разграничения ответственности за нарушения законных прав (интересов) других субъектов информационных отношений и установленных правил обращения с информацией.

В связи с этим обеспечение необходимого уровня информационной безопасности, в первую очередь персональных данных граждан, является одной из первоочередных проблем реализации программы электронного правительства.

Целями обеспечения информационной безопасности при формировании электронного правительства являются исключение или существенное уменьшение возможности нанесения субъектам электронного информационного взаимодействия материального ущерба, морального или иного случайного или преднамеренного вреда, обеспечение конфиденциальности персональных данных, служебной, профессиональной, коммерческой тайны, и сохранения устойчивого функционирования объектов информатизации органов власти, включая информационно-технологический и телекоммуникационный компонент электронного правительства.

Все информационные системы электронного правительства должны обеспечивать защиту информации от несанкционированного изменения и использовать достаточные аппаратные и программные средства обеспечения безопасности.

Информационные системы должны обеспечивать защиту от несанкционированного доступа в случаях, когда информация находится в правовом режиме тайны (конфиденциальной информации). Такая защита должна обеспечиваться в соответствии с требованиями системы информационного регулирования. Для информационных систем электронного правительства недопустимым является отсутствие механизма доступа к информации, распространение и (или) предоставление которой не ограничено в соответствии с законодательством.

Реальные достижения электронного правительства, в том числе и в области информационной безопасности, могут быть обеспечены благодаря использованию системного подхода к планированию и реализации инициатив в области электронного правительства, основанных на разработке и реализации единой архитектуры электронного правительства. Единая архитектура представляет собой структуру, отображающую взаимосвязи между всеми элементами электронного правительства и должна позволить идентифицировать и систематизировать существующие у различных министерств и ведомств потребности по использованию информационно-коммуникационных технологий на базе единых стандартов и технических решений. На различных уровнях архитектуры обеспечение безопасности может осуществляться путем аутентификации и идентификации граждан (пользователей) для доступа к тем или иным государственным информационным ресурсам (базам данных), обеспечения полноты, достоверности и целостности сведений, содержащихся и вносимых в информационные системы, защиты самих баз данных и сетей государственных органов от хищения, модификации, перехвата, защиты используемых при взаимодействии открытых каналов связи.

Однако все еще остается открытым вопрос о единой методологии формирования электронного правительства и установлении единых организационно-технических требований к его формированию и последующему существованию, в том числе и в области информационной безопасности.

Для Республики Беларусь актуальны проблемы:

создания единой системы идентификации для физических и юридических лиц;

создания государственной системы управления открытыми ключами, представляющей собой систему взаимосвязанных и аккредитованных в ней удостоверяющих и регистрационных центров;

широкомасштабного внедрения электронного документооборота и электронной цифровой подписи;

развития системы хранения государственных информационных ресурсов, используемых при оказании электронных услуг;

формирования и развития платежного шлюза в интеграции с формируемым банковской сферой единым расчетным информационным пространством;

разработки типовых политик безопасности для государственных информационных систем электронного правительства.

В результате должны быть сведены к минимуму возможности злоупотребления персональной и иной конфиденциальной информацией. Для юридических и физических лиц должны быть созданы доступные способы, механизмы и средства, обеспечивающие идентификацию и аутентификацию пользователей, конфиденциальность и целостность сообщений в системах и сетях общего пользования. Это позволит расширить сферу использования электронного документооборота, обеспечит возможности предоставления электронных услуг, широкомасштабного внедрения систем электронных платежей, иных форм многостороннего общения между населением, бизнесом и государством.

УДК 343.9(075.8)

А.И. Чурносов

ТАКТИКО-ПСИХОЛОГИЧЕСКИЕ ОСОБЕННОСТИ ПРОИЗВОДСТВА ОБЫСКА СОТРУДНИКАМИ ОРГАНОВ ПОГРАНИЧНОЙ СЛУЖБЫ

Органы пограничной службы при выполнении возложенных на них задач в местах осуществления своих полномочий имеют в соответствии с законодательством Республики Беларусь право:

осуществлять войсковые и оперативно-войсковые действия, разведывательные, оперативно-розыскные и режимные мероприятия по предупреждению, выявлению и пресечению противоправной деятельности на государственной границе;

производить личный досмотр задержанных лиц и находящихся при них вещей, досмотр транспортных средств, изымать документы, предметы и вещи, которые могут являться доказательствами совершения правонарушения, на основании и в порядке, установленных законодательством Республики Беларусь;

осуществлять самостоятельно или совместно с таможенными органами досмотр транспортных средств, следующих через государственную границу; задерживать обнаруженные при пограничном контроле товары и транспортные средства, которые перемещаются через государственную границу в нарушение установленного порядка таможенного регулирования;

досматривать транспортные средства при ведении действий по поиску и задержанию лиц, нарушивших установленный порядок пересечения государственной границы, на участках местности, где вероятно их появление;

вести дознание по делам о незаконном пересечении государственной границы;

остановить судно, произвести досмотр и задержать его, если оно не отвечает на сигналы запроса, нарушает иные правила захода в воды Республики Беларусь, плавания и пребывания в них, а также занимается промысловой и иной деятельностью в нарушение законодательства Республики Беларусь, международных договоров Республики Беларусь.

Перечисленные выше случаи осуществления сотрудниками органов пограничной службы действий, связанных с досмотром граждан, транспортных средств, хотя и не относятся к в видам обыска, однако по своей сути и природе схожи с данным следственным действием. Поэтому тактические приемы, способы и задачи обыска могут успешно использоваться органами пограничной службы в их деятельности. Знание сотрудниками органов пограничной службы тактики проведения обыска помогают повысить качество служебно-боевой деятельности при исполнении возложенных на них государством обязанностей.

Обыск – это следственное действие, направленное на обследование помещений и сооружений, участков местности, транспортных средств, отдельных граждан в целях отыскания и изъятия предметов, имеющих значение для дела, а также обнаружения разыскиваемых лиц и трупов (ст. 208, 210, 211, 212 УПК Республики Беларусь).

Производство обыска сопряжено с определенным нарушением прав граждан на неприкосновенность личности, жилища и т. п., поэтому для его проведения требуется соблюдение установленных законом гарантий.

Цели обыска:

обнаружение и изъятие предметов, имеющих доказательственное значение (орудия преступления; предметы, добытые преступным путем или на которых имеются следы преступления; документы, указывающие на важные для дела обстоятельства, а также трупы);

обнаружение разыскиваемых лиц и материалов, облегчающих их розыск (фотографии, письма, дневники);

отыскание имущества, на которое необходимо наложить арест в целях обеспечения гражданского иска или возможной конфискации.

Предметы и документы, изъятые из гражданского оборота, подлежат изъятию независимо от их отношения к делу. К их числу, в частности, относятся незарегистрированное оружие и боеприпасы к нему, взрывчатые и радиоактивные вещества, сильнодействующие яды, наркотики, порнографические издания и т. п.

Виды обыска:

– в зависимости от объектов:

обыск в помещении, находящемся в ведении (пользовании) определенных граждан либо учреждений, организаций, предприятий;

обыск на местности, которой пользуются определенные граждане;

личный обыск, заключающийся в обследовании одежды, обуви и тела человека;

обыск транспортных средств:

– с учетом последовательности производства:

первичный;

повторный.

– в зависимости от времени проведения (если необходимо произвести несколько обысков у разных лиц или у одного лица, но в разных местах, например по месту его жительства, работы, на даче):

одновременный;

неодновременный (последнее чаще всего нежелательно из тактических соображений);