конспирацию, надежную зашифровку источников (в случае необходимости), возможность проверки сообщаемых сведений и их применение только специальными субъектами.

Следует обратить внимание, что специфика деятельности оперативных подразделений ОВД вносит свои коррективы в требования, предъявляемые к оперативно-розыскной информации. В большинстве случаев последняя становится средством познания для оперативных сотрудников широкого круга социальных явлений, в том числе связанных с криминогенными процессами. Многие из этих явлений довольно полно изучены юридическими науками. Тем не менее, рассматривая их через призму ОРД, особый интерес представляют явления, порождаемые преступлением, наличие либо обнаружение которых позволяет судить о вероятности его совершения.

Ценность оперативно-розыскной информации также может заключаться в возможности отражения объективных явлений, связанных с криминогенными процессами, происходящими на обслуживаемой территории (объектах); правовой оценки действий конкретных лиц; выбора соответствующей оперативно-розыскной тактики и т. п. Приоритетное значение придается информации, позволяющей сформировать представление о способах совершения преступлений, так как это позволяет выдвигать оперативно-розыскные версии и осуществлять соответствующие оперативно-розыскные мероприятия.

Вместе с тем не всякая поступающая информация представляет ценность. Например, информация, полученная в результате противодействия преступной среды, направленная на введение в заблуждение оперативных сотрудников; добываемая лицом с недостаточным уровнем профессионального опыта; несвоевременно полученная и т. д. Данные факторы влияют на выбор и осмысление такого рода явлений, способствуют выделению наиболее значимой информации. При невозможности своевременно оценить полученную оперативно-розыскную информацию, познать ее значимость может быть потеряна наиболее существенная ее часть, а оставшаяся будет являться «информационным шумом».

В теории ОРД информация, обладающая вышеперечисленными свойствами, определяется термином «оперативно значимая информация», возникновению которой предшествуют активные действия оперативных сотрудников по ее выявлению. В качестве элементов этих действий выделяют сбор первичной информации, ее предварительный анализ на предмет отнесения к оперативно-розыскной информации и уже в последующем анализ и проверку, позволяющие выделить оперативно значимую информацию, дающую основания для принятия оперативно-розыскных решений.

Таким образом, представляется возможным сделать вывод о том, что оперативно значимая информация является результатом трансформации оперативно-розыскной информации в процессе ее аналитической обработки и сопоставления с другими оперативными данными, поступающими из различных источников. Ее наличие позволяет оперативным сотрудникам устанавливать предметы, которые могут быть вещественными доказательствами (финансовые документы, товарно-материальные ценности, денежные средства и т. д.), места их хранения (сокрытия), способы вывода и легализации, что в целом отражает механизм реализации преступных замыслов, прямо или косвенно указывает на наличие состава противоправного деяния в действиях конкретных лиц.

УДК 342

А.А. Подупейко

НЕКОТОРЫЕ ВОПРОСЫ ЦИФРОВИЗАЦИИ В ОРГАНАХ ВНУТРЕННИХ ДЕЛ РЕСПУБЛИКИ БЕЛАРУСЬ

Современное развитие мирового сообщества требует постоянного совершенствования деятельности во всех сферах общественных отношений. Это обусловлено стремительным развитием информационно-цифровых технологий, которые стали основой функционирования различных субъектов в большинстве сфер деятельности. И государственные организации, и учреждения, и частные компании сегодня ставят цифровизацию в ряд своих основных и стратегических приоритетов для достижения устойчивого конкурентного преимущества в отрасли.

В Государственной программе развития цифровой экономики и информационного общества на 2016–2020 годы закреплено, что в Республике Беларусь процесс цифровой трансформации рассматривается как один из важнейших факторов обеспечения конкурентоспособности и инновационного развития как отдельных организаций, так и национальной экономики в целом.

Граждане также стали зависеть от информационных технологий. Они значительное количество времени проводят в социальных сетях. Смартфоны, планшеты, персональные компьютеры превратились в персональные центры управления каждого человека. При этом пользователи стремятся получить немедленно не только какие-либо сведения, но и товар или услуги.

При всех положительных и созидательных моментах информационно-цифровые технологии используются и для достижения негативных целей. Распространяется практика целенаправленного информационного давления, наносящего существенный ущерб как интересам отдельных учреждений и организаций, так и национальным интересам государства в целом.

Злоумышленники атакуют личные аккаунты граждан, сайты государственных органов, в том числе правоохранительных, преследуя при этом совершенно разные цели и интересы. Целью может быть похищение информации или демонстрация, насколько плохо защищен сайт органа, данные о служебной деятельности, конфиденциальные данные сотрудников, персональные данные граждан и др. Беспокойство вызывает также активное распространение в информационном пространстве фальсифицированной и недостоверной информации. Это создает предпосылки для преднамеренной дестабилизации устоявшихся общественных отношений.

Процессы глобализации, возникающие различные общественные вызовы и угрозы, цифровизация общества и, как результат, изменяющееся сознание и социальное поведение людей, а также цифровая трансформация учреждений, организаций, предприятий и компаний актуализируют необходимость корректировки деятельности и органов внутренних дел Республики Беларусь.

Как показывает практика, в процессе выполнения возложенных задач (ст. 2 Закона от 17 июля 2007 г. № 263-З «Об органах внутренних дел Республики Беларусь») по обеспечению интересов личности, общества и государства, именно органы внутренних дел в первую очередь противодействуют внешним угрозам и иным посягательствам в сфере информационно-коммуникационных технологий.

Органы внутренних дел, как и все общество в целом, для того чтобы соответствовать современным тенденциям развития и не отстать, должны внедрять и использовать в своей деятельности цифровые технологии, а также повышать профессиональный уровень своих сотрудников в информационной сфере.

Следует отметить, что органы внутренних дел уже давно и успешно используют в своей деятельности современные информационно-коммуникационные технологии. Специфика деятельности такова, что органы внутренних дел активно противодействуют преступлениям с использованием IT-технологий, например несанкционированному доступу к личным данным граждан – взламыванию аккаунтов пользователей в социальных сетях, электронных кошельков и почтовых ящиков, систем дистанционного банковского обслуживания и др.

Безусловно, должны быть предприняты необходимые меры по эффективному противодействию киберугрозам и совершенствованию деятельности. Движение по этому пути требует перестройки различных процессов, прежде всего организационных. Должна быть выработана, на наш взгляд, комплексная цифровая концепция развития органов и подразделений внутренних дел, которая предусматривала бы вопросы цифровой трансформации и затраты на ее осуществление, организационно-управленческие мероприятия, внедрение новых информационных технологий, подготовку и повышение квалификации сотрудников в области цифровизации и т. д. Должны быть определены приоритетные сферы защиты информации, и в этом случае могут иметь место различные уровни защиты той или иной информации или технологий.

Велика роль в этом процессе руководства органа. Руководство должно осознавать возможности цифровизации и понимать ее необходимость. Полагаем, что организовывать цифровизацию органа должен один из руководителей. При этом он должен быть современным и мыслить современно, обладать разносторонними знаниями. Он должен быть стратегом, принадлежать к «цифровому поколению» и хорошо понимать потребности и задачи органа внутренних дел и сотрудников. Более того, он долен отлично разбираться в цифровых технологиях, мыслить, как предприниматели, действовать гибко и оперативно, обладать необходимыми компетенциями.

Важнейшей задачей, на наш взгляд, является обучение и инструктирование сотрудников правилам информационной безопасности при работе с компьютерной техникой, носителями цифровой информации, мобильными устройствами связи, а также при использовании электронной почты и других интернет-сервисов, особенно бесплатных почтовых сервисов.

В связи с этим должна быть скорректирована система подготовки кадров и повышения квалификации. В тематике соответствующих образовательных курсов должны найти отражение вопросы цифровизации деятельности самих органов внутренних дел, нормы и правила информационной безопасности, современные дестабилизирующие факторы и угрозы, особенности защиты информации служебного характера, персональных сведений о гражданах, а также меры ответственности в случаях допущения нарушений законодательства. В качестве приоритета развития компетенций в данной области можно выделить такие, как умение работать в интегрированных информационно-аналитических системах; четкое следование правилам информационной безопасности; соблюдение требований по защите служебной информации и т. д. Целесообразно, по нашему мнению, к образовательному процессу привлекать практических сотрудников, которые непосредственно занимаются противодействием киберпреступлениям.

Формирование цифровой компетентности сотрудника органов внутренних дел – одно из основных и важнейших требований современности. Овладение новейшими формами информационного обеспечения деятельности в некоторых случаях позволяет выявлять и раскрывать преступления, не выходя из служебного кабинета.

Сегодня действительность такова, что каждый сотрудник должен уметь пользоваться электронным документооборотом, служебной почтой, использовать базы данных и информационные ресурсы органов внутренних дел и других государственных органов, а также современные цифровые технологии и программный продукт, владеть навыками в области информационной безопасности и защиты информации.

УДК 341.244

П.В. Прохоров

РЕАЛИЗАЦИЯ МЕЖДУНАРОДНЫХ ДОГОВОРОВ В ОПЕРАТИВНО-СЛУЖЕБНОЙ ДЕЯТЕЛЬНОСТИ

Согласно абзацу тринадцатому части первой ст. 1 Закона Республики Беларусь от 23 июля 2008 г. № 421-З «О международных договорах Республики Беларусь» международный договор в Республике Беларусь может быть межгосударственным, межправительственным или международным договором межведомственного характера, заключенным Республикой Беларусь не только с иностранным государством (государствами), но и с международной организацией (организациями), иным субъектом (субъектами), независимо от способа заключения (подписание, обмен нотами, письмами или иными документами, образующими международный договор, ратификация, утверждение (принятие), присоединение). В зависимости от органов, представляющих государство, различают межгосударственные, межправительственные и межведомственные договоры.

Межгосударственные договоры – международные договоры, которые заключаются с иностранными государствами, а также с международными организациями и иными образованиями от имени Республики Беларусь. Такие договоры заключаются на высшем уровне главой государства либо специально уполномоченным им лицом. Наиболее значимые межгосу-