Certain issues of qualification of crimes under Art. 430-432 of the Criminal Code of the Republic of Belarus. Based on the legislation, the analysis of scientific literature and law enforcement practice, their own opinions and suggestions were made on a number of aspects of a debatable nature.

Keywords: bribery, qualification of receiving a bribe, qualification of giving a bribe, qualification of mediation in bribery.

УДК 342.95

***М.В. Губич**, кандидат юридических наук, заместитель начальника кафедры правовой информатики Академии МВД Республики Беларусь*
(e-mail: gubichmv@yandex.by)

СОВРЕМЕННОЕ СОСТОЯНИЕ И ПРОБЛЕМЫ ПРАВОВОГО РЕГУЛИРОВАНИЯ ГОСУДАРСТВЕННО-ЧАСТНОГО ПАРТНЕРСТВА В СФЕРЕ ПРОТИВОДЕЙСТВИЯ КИБЕРПРЕСТУПНОСТИ

Проанализированы нормативные правовые акты, регламентирующие государственно-частное партнерство в сфере противодействия киберпреступности. Проведена оценка современного состояния рассматриваемой деятельности, выявлен ряд проблем в правовом и организационном обеспечении данной формы взаимодействия. Акцентируется внимание на отсутствии в законодательстве Республики Беларусь нормативных правовых актов, осуществляющих специфическое регурирование государственно-частного партнерства в сегменте обеспечения информационной безопасности и противодействия киберпреступности. Предлагаются меры по совершенствованию государственно-частного партнерства в сфере противодействия киберпреступности, выделены основные области применения механизмов по осуществлению взаимодействия коммерческих организаций и правоохранительных органов для противодействия киберугрозам.

Ключевые слова: государственно-частное партнерство, информационная безопасность, противодействие киберпреступности.

Одним из относительно новых правовых образований в национальном законодательстве является институт государственно-частного партнерства – один из приоритетов экономической политики. Необходимость его формирования и реализации посредством него проектов, имеющих особое социальное значение, предполагает сотрудничество правоохранительных органов и субъектов хозяйственной, финансовой и иной коммерческой деятельности по вопросам обеспечения противодействия киберпреступности.

Правовой регламентации взаимовыгодного сотрудничества государства и бизнеса законодателем уделялось внимание уже на первых этапах становления национальной нормативной правовой базы: в 1991 г. парламентом приняты Законы Республики Беларусь «Об инвестиционной деятельности в Республике Беларусь» и «Об иностранных инвестициях на территории Республики Беларусь». Спустя десять лет вступил в силу Инвестиционный кодекс Республики Беларусь, установивший порядок осуществления инвестиционной деятельности, а также принята Программа деятельности Правительства Республики Беларусь на 2011–2015 годы, в которой государственно-частное партнерство отнесено к числу основных направлений деятельности Правительства Республики Беларусь. Результатами выполнения указанной программы явилось: принятие Законов Республики Беларусь «Об инвестициях» и «О концессиях», также разработка и принятие Закона Республики Беларусь от 30 декабря 2015 г. № 345-З «О государственно-частном партнерстве»; создание межведомственного инфраструктурного координационного совета (органа, созданного для координации вопросов долгосрочного развития объектов инфраструктуры, в том числе в рамках государственно-частного партнерства); разработка и утверждение решением указанного совета Национального инфраструктурного плана на 2016–2030 гг., отражающего инфраструктурную потребность страны и разрыв бюджетного финансирования на долгосрочную перспективу.

Таким образом, можно отметить, что в настоящее время в Республике Беларусь создана законодательная база государственно-частного партнерства (по состоянию на 11 февраля 2020 г. рассматриваемый правовой институт регламентирован 197 нормативными актами), сформирована институциональная среда и реализуются первые пилотные проекты.

Тенденцию к увеличению внимания к государственно-частному партнерству при построении государственной политики в сфере обеспечения национальной безопасности можно проследить на примере анализа содержания документов, закрепляющих официальные взгляды на сущность и содержание деятельности Республики Беларусь по обеспечению национальной безопасности, в том числе

в информационной сфере, – Концепции национальной безопасности Республики Беларусь, утвержденной Указом Президента Республики Беларусь от 9 ноября 2010 г. № 575, и Концепции информационной безопасности Республики Беларусь, утвержденной постановлением Совета Безопасности Республики Беларусь от 18 марта 2019 г. № 1. Так, если в первом документе расширение практики и совершенствование механизмов государственно-частного партнерства рассматривается в качестве инструмента, обеспечивающего повышение созидательной активности населения и основы формирования и развития гражданского общества (п. 49), то во втором – данной форме сотрудничества посвящена целая глава (гл. 26).

К основным задачам государственно-частного партнерства относится создание условий для обеспечения национальной безопасности Республики Беларусь, а также совершенствование инженерно-технических средств защиты, средств и систем охраны, используемых для предупреждения и выявления противоправной деятельности. К сферам осуществления рассматриваемого сотрудничества законодательством отнесены электросвязь, правоохранительная деятельность, информационные и телекоммуникационные технологии и т. д.

Проанализировав содержание национальных нормативных правовых актов, относительно рассматриваемого вопроса можно отметить следующее:

законодателем представлены необходимые правовые основания для осуществления государственно-частного партнерства в сфере противодействия киберпреступности;

данная форма сотрудничества признана наиболее эффективной моделью обеспечения информационной безопасности, что в полной мере относится и к области противодействия киберпреступности;

основными целями рассматриваемой формы взаимодействия являются привлечение квалифицированных кадров, технологий, капитала частных предприятий, повышение эффективности использования бюджетных средств;

государство заинтересовано в развитии механизмов противодействия киберпреступлениям.

Анализ деятельности подразделений по раскрытию преступлений в сфере высоких технологий показывает, что в ходе решения задач противодействия киберпреступности органы внутренних дел испытывают потребность в квалифицированных специалистах в области информационных технологий, специальном программном обеспечении, дорогостоящих технических комплексах и т. п. В условиях государственного финансирования рассматриваемой деятельности и имеющихся бюджетных ограничений удовлетворение указанных потребностей без привлечения дополнительных значительных финансовых инвестиций практически невозможно. Вместе с тем национальный сегмент коммерческих компаний, специализирующихся по вопросам оказания услуг в сфере обеспечения информационной безопасности, имеет определенный опыт и технические решения в областях обнаружения и противодействия вредоносным техническим воздействиям на компьютерные системы и сети, анализа происшедших киберинцидентов и фиксации электронных доказательств. При этом данные организации не только показывают высокую эффективность, но и заинтересованы в расширении своей деятельности.

В контексте настоящего исследования представляется интересным отметить опыт Российской Федерации (Доктрина информационной безопасности Российской Федерации, утверждена Указом Президента Российской Федерации от 5 декабря 2016 г. № 646, в соответствии с законодательством которой к субъектам, являющимся участниками системы обеспечения информационной безопасности, отнесены собственники объектов критической информационной инфраструктуры и организации, эксплуатирующие такие объекты, средства массовой информации, организации денежно-кредитной, банковской и иных сфер финансового рынка, операторы связи и информационных систем, организации, осуществляющие деятельность по созданию и эксплуатации информационных систем и сетей связи, по производству и эксплуатации средств обеспечения информационной безопасности, по оказанию услуг в области информационной безопасности, организации, осуществляющие образовательную деятельность в данной области, общественные объединения, иные организации и граждане, которые участвуют в решении задач по обеспечению информационной безопасности.

В этой связи представляется обоснованным полагать, что такие коммерческие организации могут быть задействованы в деятельности по обеспечению информационной безопасности Республики Беларусь, тем более, что правовые основания для этого предоставлены Концепцией обеспечения национальной безопасности, в соответствии с которой граждане, общественные и иные организации наравне с государством отнесены к субъектам обеспечения национальной безопасности (п. 45).

В этой связи основой Концепции противодействия киберпреступности посредством применения механизмов государственно-частного партнерства выступает положение о том, что развитие

инфраструктурных объектов, созданных посредством данного механизма, способствует снижению издержек государственных субъектов информационной безопасности. Соответственно, изучаемую форму взаимодействия государства и бизнеса следует рассматривать как стратегический фактор повышения защищенности национальных интересов в информационной сфере.

Вместе с тем до настоящего времени отсутствует информация о реализации в Республике Беларусь инфраструктурных проектов в исследуемой сфере. Представляется, что указанная ситуация обусловлена в первую очередь тем, что законодателем не была учтена специфика различных отраслей, в которых возможна реализация проектов государственно-частного партнерства, в том числе специфика осуществления правоохранительной деятельности в сегменте обеспечения информационной безопасности и противодействия киберпреступности.

Существенным проблемным аспектом в правовом регулировании государственно-частного партнерства является отсутствие в законодательстве положений, регламентирующих вопросы, связанные с созданием информационно-коммуникационной инфраструктуры, разработкой и внедрением информационных и телекоммуникационных технологий, посредством которых будут протекать информационные процессы с использованием сведений, образующихся в процессе осуществления правоохранительной деятельности, и иной информации, распространение и (или) предоставление которой ограничено. Разрешение данного проблемного аспекта особенно значимо для практики государственно-частного партнерства в сфере противодействия киберпреступности по причинам циркуляции огромных объемов данных, содержащих в себе охраняемую законом информацию, а также тяжести последствий, которые могут наступить в результате разглашения или утраты такой информации.

В этой связи отсутствие специфического регулирования является существенным сдерживающим фактором, ограничивающим возможности развития механизмов государственно-частного партнерства, востребованных как в целом в сфере обеспечения информационной безопасности, так и в области противодействие киберпреступности.

Следует отметить, что в развитии сотрудничества государства и коммерческих организаций первое является наиболее заинтересованным, так как при частном финансировании инфраструктурных объектов решаются государственно важные задачи в сфере противодействия киберпреступности, при этом государство сохраняет за собой контроль за деятельностью таких объектов. Однако на официальном сайте Министерства экономики Республики Беларусь (наделено наиболее широкими компетенциями в части реализации единой государственной политики в сфере государственно-частного партнерства и координации рассматриваемой деятельности) в разделе «Государственно-частное партнерство в Республике Беларусь» среди основных направлений развития инфраструктуры с применением рассматриваемого механизма взаимодействия не значатся такие сферы, как электросвязь, правоохранительная деятельность, информационные и телекоммуникационные технологии, что, по нашему мнению, является фактором, в определенной степени препятствующим сотрудничеству коммерческих компаний и правоохранительных органов в сфере противодействия киберпреступности.

Необходимо также подчеркнуть, что и на сайте МВД Республики Беларусь также отсутствует информация о готовности ведомства к взаимовыгодному сотрудничеству с общественными и коммерческими организациями в форме государственно-частного партнерства для решения задач, возложенных на органы внутренних дел, в том числе противодействия правонарушениям по направлению деятельности подразделений по раскрытию преступлений в сфере высоких технологий.

В рамках рассматриваемого вопроса представляется возможным подвергнуть критике состав межведомственного инфраструктурного координационного совета, в число членов которого не включены представители правоохранительных органов. Негативным следствием этого явилось отсутствие в Национальной инфраструктурной стратегии Республики Беларусь в 2017–2030 гг. как проектов в правоохранительной сфере в целом, так и в сфере противодействия киберпреступности в частности.

Вместе с тем, несмотря на отмеченные негативные факторы, обоснованно и логично отметить инициативные шаги по развитию государственно-частного партнерства, предпринимаемые МВД Республики Беларусь. Решением коллегии данного правоохранительного ведомства от 31 января 2020 г. № 2км предписано основные усилия органов внутренних дел в текущем году сосредоточить на реализации новых подходов к организации оперативно-служебной деятельности, а подразделениям по раскрытию преступлений в сфере высоких технологий указано на необходимость осуществления мер по совершенствованию государственно-частного партнерства по противодействию противоправным деяниям по направлению деятельности данных подразделений органов внутренних дел.

Исходя из анализа приведенного в исследовании материала и практики деятельности подразделений по раскрытию преступлений в сфере высоких технологий органов внутренних дел, видится

возможным выделить следующие перспективные области применения механизмов государственно-частного партнерства в сфере противодействия киберпреступности, что включает:

участие специалистов в проведении оперативно-розыскных мероприятий и следственных действий, обследовании компьютерных систем, сборе и анализе цифровых доказательств, в том числе проведении компьютерно-технических экспертиз;

разработку и внедрение специального программного обеспечения, позволяющего выявлять киберугрозы, проведение консультирования и аудита систем обеспечения информационной безопасности организаций различных форм собственности;

осуществление мониторинга киберпространства в целях выявления вредоносного трафика и программного обеспечения, запрещенной к распространению информации, а также развитие и внедрение технологий анализа Больших Данных.

Таким образом, проведенный анализ законодательства позволяет заключить, что в Республике Беларусь создана правовая основа для решения задач противодействия киберпреступности в форме государственно-частного партнерства. Государство заинтересовано в реализации проектов рассматриваемой формы взаимодействия. Вместе с тем имеются правовые и организационные проблемы реализации проектов государственно-частного партнерства в сфере противодействия киберпреступности. В этой связи представляется обоснованным и актуальным проведение дальнейших научных исследований, направленных на разработку научной концепции государственно-частного партнерства в рассматриваемой сфере, а также подготовку предложений по совершенствованию ее организационного и правового обеспечения.

Дата поступления в редакцию: 19.02.20

M.V. Gubich, *Candidate of Juridical Sciences, Deputy Head of the Department of Legal Informatics of the Academy of the MIA of the Republic of Belarus*

CURRENT STATE AND PROBLEMS OF LEGAL REGULATION OF PUBLIC-PRIVATE PARTNERSHIP IN THE SPHERE OF COMBATING CYBERCRIME

Normative legal acts regulating public-private partnership in the sphere of combating cybercrime are analyzed. An assessment of the current state of the considered activity has been made, and a number of problems in the legal and organizational support of this form of interaction have been identified. The article focuses on the absence of normative legal acts in the legislation of the Republic of Belarus that carry out specific regulation of public-private partnership in the sphere ensuring information security and combating cybercrime. Measures to improve public-private partnership in the sphere of combating cybercrime are proposed, and the main areas of application of mechanisms for interaction between commercial organizations and law-enforcement agencies for combating cyber threats are highlighted.

Keywords: public-private partnership, information security, combating cybercrime.

УДК 343.982

В.И. Елётнов*, кандидат юридических наук, старший преподаватель кафедры криминалистических экспертиз следственно-экспертного факультета Академии МВД Республики Беларусь*
(e-mail: v.eletnov@mail.ru);
В.А. Чванкин*, кандидат юридических наук, доцент, доцент кафедры криминалистических экспертиз следственно-экспертного факультета Академии МВД Республики Беларусь*
(e-mail: tanvad@mail.ru)

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ, ИСПОЛЬЗУЕМОЕ ПРИ ПРОВЕДЕНИИ СУДЕБНОЙ ПОРТРЕТНОЙ ЭКСПЕРТИЗЫ: ОБЩАЯ ХАРАКТЕРИСТИКА И СРАВНИТЕЛЬНЫЙ АНАЛИЗ

Анализируется состояние обеспеченности судебной портретной экспертизы различными программными продуктами. Описываются содержание, ход и результаты проведенного авторами сравнительного исследования возможностей отдельных графических и текстовых редакторов общего назначения, используемых экспертами при проведении судебной портретной экспертизы, используются методы детального исследования: визуального сопоставления признаков с их последующей разметкой, сопоставления с использованием масок, сопоставления с помощью наложения координатных сеток, сопоставления относительных величин и др. Приводятся сведения об альтернативных, свободно распространяемых графических редакторах, возможностях их использования в рамках судебной портретной экспертизы. Рассматриваются возможности специализированных