

временных упреждающих мер по ограничению эскалации негативных явлений и процессов в социально-экономической сфере страны.

В целях повышения уровня независимости государственного контроля исходя из положений ст. 25 Лимской декларации руководящих принципов контроля предлагается:

введение в Республике Беларусь института несменяемости высших должностных лиц органов государственного контроля с использованием, например, модели, применяемой к членам Конституционного Суда Республики Беларусь;

сужение возложенных на него полномочий рамками защиты финансовых и иных государственных средств;

повышение уровня доступности информации о результатах деятельности органов государственного контроля для юридических и физических лиц.

Важными направлениями повышения эффективности надзора исполнительной власти Республики Беларусь могут стать: увеличение доли надзорных функций за счет снижения контрольных применительно ко всем государственным и негосударственным предприятиям, учреждениям и организациям, с одной стороны, и усиление их правовой ответственности за нарушение законодательства – с другой; внесение в законодательство Республики Беларусь изменений и дополнений, закрепляющих надзорные функции органов исполнительной власти.

УДК 347

М.В. Войтеховская, Т.В. Прохоренко

СОВЕРШЕНСТВОВАНИЕ ПРАВОВОГО РЕГУЛИРОВАНИЯ В СФЕРЕ ГОСУДАРСТВЕННЫХ ЗАКУПОК ТОВАРОВ (РАБОТ, УСЛУГ) КАК ЭФФЕКТИВНЫЙ ИНСТРУМЕНТ ОБЕСПЕЧЕНИЯ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ РЕСПУБЛИКИ БЕЛАРУСЬ

Тема государственных закупок товаров (работ, услуг) в Республике Беларусь (далее – государственные закупки) традиционно является одной из актуальных в сфере обеспечения экономической безопасности государства.

Государственные закупки – необходимый элемент экономической безопасности государства, поскольку они связаны с функционированием бюджетного сектора в экономике, с помощью которого финансируются в том числе различные отрасли государственного управления, культура, образование, здравоохранение и др.

Экономическая безопасность в сфере государственных закупок обеспечивается рациональным расходованием средств бюджета, достиганием высокого качества поставляемых товаров, выполняемых работ, оказываемых услуг, преобладанием конкурентных процедур при определении (выборе) поставщиков (подрядчиков, исполнителей).

Предмет государственной закупки – товары (работы, услуги), определенные заказчиком для приобретения в рамках процедуры государственной закупки. К предмету закупки, в частности, могут относиться: различного рода техника, в том числе спецтехника, автотранспорт, горюче-смазочные материалы; работы по строительству зданий и сооружений как гражданского, так и оборонного характера, строительству жилого фонда государственного назначения; оборудование, полиграфическая продукция, мебель, канцелярские товары для государственных учреждений, а также оказание им строительно-ремонтных услуг; товары и их поставка и др.

1 июля 2019 г. вступила в силу редакция Закона Республики Беларусь от 17 июля 2018 г. № 419-З «О государственных закупках товаров (работ, услуг)» (далее – Закон), которой предусмотрены существенные изменения в правовом регулировании сферы государственных закупок. Особое внимание обращено на антикоррупционные меры. Повышены гласность и прозрачность процесса организации и проведения процедур государственных закупок, введены новые инструменты оперативного реагирования на выявленные нарушения.

Поскольку Республика Беларусь взяла курс на развитие электронного государства, значительная часть Закона посвящена нормам, регулирующим процедуру закупок при их размещении на электронной торговой площадке (<https://goszakupki.by/>). С одной стороны, такая процедура обеспечивает прозрачность проводимых закупок, с другой – возникают проблемы, связанные с недостаточным правовым регулированием и фактическим применением существующих норм.

Так, имеются сложности при заключении договора в электронном виде посредством электронного документа с использованием электронной цифровой подписи. При такой процедуре повышается риск оспаривания второй стороной факта заключения договора или согласования его отдельных условий. В отличие от стандартного подписания договора представителями его сторон при заключении договора путем направления документов в электронном виде через электронную торговую площадку вторая сторона с большей степенью вероятности может утверждать, что она не заключала договор, так как, например, аналогом собственноручной подписи руководителя (иного уполномоченного

представителя) воспользовался некий сотрудник, не имея на то согласия уполномоченного лица, либо отдельные условия договора согласовывало не уполномоченное, а иное лицо, которое воспользовалось аналогом собственноручной подписи руководителя (уполномоченного представителя), не имея на то согласия уполномоченного лица.

К тому же, как показывает судебная практика, часто суд не принимает договор, заключенный в электронном виде, требуя его бумажный вариант. Сложности возникают и внутри государственных организаций, поскольку, например, бухгалтерия также требует бумажный вариант заключенного на электронной торговой площадке договора как доказательство того, что он подписан обеими сторонами и имеет юридическую силу.

Таким образом, в правовом регулировании в сфере государственных закупок, в реализации отдельных норм и положений Закона, других нормативных правовых актов имеются проблемы, которые отрицательно влияют на экономику отдельных государственных предприятий и страны в целом. Вместе с тем государственные закупки представляют собой эффективный инструмент обеспечения экономической безопасности государства. Внедрение в Республике Беларусь «электронного государства» требует решения ряда проблем, возникающих в ходе реализации существующих норм и положений. Информационное общество, несмотря на определенные трудности, стремится к простому, быстрому и комфортному взаимодействию с государством и, в свою очередь, помогает государству решать различные проблемы и задачи, т. е. повышать благосостояние нации.

УДК 004.056

С.Ю. Воробьев, Д.А. Жук, В.А. Русак, В.А. Шкред

ОСОБЕННОСТИ КИБЕРПРЕСТУПЛЕНИЙ В БАНКОВСКОМ СЕКТОРЕ

В эпоху стремительного развития технологий практически все сферы жизнедеятельности человека подверглись цифровой трансформации. Появились такие правонарушения, которые получили общее название «киберпреступность». Кража данных доступа к системе интернет-банкинга, а также банковских платежных карточек (банковских счетов) с целью завладения средствами клиентов банка, кража персональных данных и коммерческой информации из частных компьютеров или серверов, умышленное повреждение информационных систем или средств коммуникации с целью создания убытков компаниям – часть подобных угроз, связанных с бурным развитием информационных технологий.

Опасность киберпреступлений в банковском секторе связана с тем, что цифровые технологии развиваются стремительно и злоумышленники изобретают новые способы обхода систем безопасности, к которым имеющиеся системы защиты не готовы. Киберпреступления, как и другие виды преступлений, совершаются одним или несколькими правонарушителями, как правило, обладающими колоссальными знаниями в области цифровых технологий, используемыми для достижения корыстных целей. Наиболее привлекательным для таких преступников является банковский сектор, в котором ежедневно происходит множество транзакций и осуществляется оборот огромного количества денежных средств.

Так, в поле зрения злоумышленников и международных преступных группировок находится банковская система Республики Беларусь. В последние несколько лет постоянно выявлялись факты мошенничества с использованием электронных платежных средств, имели места хакерские атаки на банки Республики Беларусь, в результате которых злоумышленники похищали значительные денежные средства. Сотрудниками правоохранительных органов на территории Республики Беларусь задерживались участники международных преступных группировок Cobalt, Andromeda и др.

Анализ мировой практики правоохранительной деятельности позволяет выделить следующие наиболее характерные для банковской сферы виды киберугроз:

воздействие через аппаратные уязвимости, которые имеются в микропроцессорах разных производителей и не устраняются при помощи программных обновлений, но открывают новые возможности для злоумышленников;

компьютерный шпионаж, направленный на долговременное присутствие в сетях объектов критической информационной инфраструктуры с целью саботажа и слежения за деятельностью финансовых организаций;

целенаправленные кибератаки на конкретные финансовые организации, позволяющие злоумышленникам проникать в сеть организаций и далее к изолированным финансовым системам для вывода денежных средств;

клиентоориентированные кибератаки, направленные непосредственно на клиентов банков, а именно на хищение их денежных средств.

Типовая схема таргетированной кибератаки на банк состоит из следующих этапов:

массовая рассылка писем на e-mail работников банка, в которых содержится вредоносное программное обеспечение;

внедрение вредоносного программного обеспечения при открытии письма работником банка для установки доступа к зараженному компьютеру;