УДК 004.056

ПРАВОВОЕ РЕГУЛИРОВАНИЕ КИБЕРБЕЗОПАСНОСТИ В УСЛОВИЯХ РАЗВИТИЯ ЦИФРОВОЙ ЭКОНОМИКИ

Е. С. Ковалёнок
Белорусский государственный экономический университет

Аннотация

В статье анализируется нормативно-правовое регулирование обеспечения кибербезопасности в иностранных государствах и в национальной правовой системе, структура и организационное построение обеспечивающих ее органов за рубежом. Высказывается предложение о совершенствовании национального законодательства в условиях цифровой трансформации общества и государства.

Ключевые слова: кибербезопасность, национальная безопасность, информационная безопасность, информационно-коммуникационные технологии, цифровая экономика, правовое регулирование.

Цифровая трансформация экономики становится все более значимой в жизни нашего общества. К 2025 г. государство намерено обеспечить внедрение информационно-коммуникационных и передовых производственных технологий в отрасли национальной экономики и сферы жизнедеятельности общества. С этой целью утверждена Государственная программа «Цифровое развитие Беларуси» на 2021–2025 годы, формирование которой осуществлялось с учетом Стратегии развития информатизации в Республике Беларусь на 2016−2022 годы, а также законодательства, регулирующего вопросы информатизации, создания информационных технологий, систем и сетей, обеспечения защиты информации, а также результатов научных исследований, практического опыта создания и развития информационно-коммуникационных технологий. В рамках программы предусматривается выполнение мероприятий по созданию современной информационно-коммуникационной инфраструктуры, внедрению цифровых инноваций в отраслях экономики и технологий «умных городов», а также обеспечению информационной безопасности таких решений. Выполнение предусмотренных программой мероприятий требует адаптации действующего и разработки нового законодательства, которое устранит пробелы, барьеры, препятствующие развитию цифровой экономики, создаст благоприятную правовую основу для дальнейшего развития цифровых технологий и их внедрения в отрасли экономики.

Для заполнения возможных пробелов в отечественном законодательстве следует изучить зарубежный опыт правового регулирования соответствующих правоотношений.

Например, в Российской Федерации приняты следующие нормативные правовые акты, устанавливающие организационные и правовые основы

функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак:

Указ Президента Российской Федерации от 3 февраля 2012 г. № 803 «Основные направления госполитики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации». Данным документом вводится понятие единой государственной системы обнаружения и предупреждения компьютерных атак на критически важную информационную инфраструктуру, в том числе дается определение силам и средствам обнаружения и предупреждения атак, а также силам и средствам ликвидации последствий инцидентов;

Указ Президента Российской Федерации от 15 января 2013 г. № 31–С «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации». Данный Указ инициирует создание государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак, определяет основные задачи системы.

Опыт Российской Федерации в сфере установления ответственности за нарушение безопасности критической информационной инфраструктуры показывает, что страна идет по пути ужесточения наказания за такие нарушения. В зависимости от тяжести последствий предусмотрена ответственность вплоть до лишения свободы на срок от шести до десяти лет.

Для обеспечения информационной безопасности федеральных информационных систем и организаций в Соединенных Штатах Америки обязательны для выполнения требования следующих документов: Закона «Federal Information Security Management Act of 2002 (Public Law 107-347)»; стандарта NIST 800-137 от 30 сентября 2011 г. «Information Security Continuous Monitoring for Federal Information Systems and Organizations». Основной задачей данного стандарта является организация непрерывного мониторинга информационной безопасности в целях реагирования на постоянно изменяющиеся угрозы в сфере информационной безопасности; стандарта NIST 800-61 от 6 августа 2012 г. «Computer Security Incident Handling Guide». Стандарт определяет порядок реагирования и предотвращения инцидентов информационной безопасности, создания групп реагирования на инциденты, а также регламент ее функционирования.

27 июня 2019 г. в Европейском союзе вступил в силу Закон «О кибербезопасности», в соответствии с которым Агентство Европейского союза по кибербезопасности (ENISA) наделено новыми полномочиями и создана европейская система сертификации кибербезопасности. Кроме того, данное агентство выступает в качестве секретариата национальных групп реагирования на компьютерные инциденты. 6 июля 2016 г. Европейским агентством по сетевой и информационной безопасности разработана директива «NIS Directive» по повышению безопасности сетей и информационных систем, которая устанавливает требования по информационной безопасности для операторов критически важных услуг и провайдеров цифровых услуг. Директива является

первой частью общеевропейского законодательства о кибербезопасности, ее цель – повышение кибербезопасности в Европейском союзе. Директива предъявляет требования ко всем 28 членам Евросоюза, в том числе Правительство каждой страны обязано соблюдать указанные в ней требования и создать собственный центр реагирования на инциденты, связанные с кибербезопасностью;

С целью недопущение официально беспрецедентных попыток кибератак на органы государственного управления, государственные организации и информационную инфраструктуру Республики Беларусь и, как следствие, возникновения рисков и угроз национальным интересам в информационной сфере (что особенно остро проявилось в электоральный период 2020 г. и постэлекторальный 2021 год), полагаясь на опыт зарубежных стран, видится возможным разработка нормативного правового акта, который будет способствовать комплексному регулированию вопросов обеспечения информационной безопасности. В соответствии Законом Республики Беларусь от 17 июля 2018 г. № 130-З «О нормативных правовых актах» требуется правовое регулирование общественных отношений, ранее не урегулированных, и имеющиеся проблемы не могут быть разрешены без принятия (издания) нормативного правового акта.

Данный акт обеспечил бы дальнейшую реализацию положений, определенных в постановлении Совета Безопасности Республики Беларусь от 18 марта 2019 г. № 1 «О Концепции информационной безопасности Республики Беларусь», по формированию комплексного подхода по обеспечению кибербезопасности Республики Беларусь в информационной сфере в части регулирования вопросов, касающихся автоматизированного контроля состояния кибербезопасности информационной инфраструктуры государства.

При подготовке проекта нормативного правового акта следует провести анализ следующих актов законодательства: Закона Республики Беларусь от 10 ноября 2008 г. № 455-З 2Об информации, информатизации и защите информации»; Закона Республики Беларусь от 19 июля 2010 г. № 170-З «О государственных секретах»; Указа Президента Республики Беларусь от 16 октября 2009 г. № 510 «О совершенствовании контрольной (надзорной) деятельности в Республике Беларусь»; Указа Президента Республики Беларусь от 1 сентября 2010 г. № 450 «О лицензировании отдельных видов деятельности»; Указа Президента Республики Беларусь от 9 ноября 2010 г. № 575 «Об утверждении Концепции национальной безопасности Республики Беларусь»; постановления Совета Безопасности Республики Беларусь от 18 марта 2019 г. № 1 «О Концепции информационной безопасности Республики Беларусь»; Указа Президента Республики Беларусь от 16 апреля 2013 г. № 196 «О некоторых мерах по совершенствованию защиты информации» и принятых в его развитие нормативных правовых актов ОАЦ и других нормотворческих органов.

Учитывая массив национального законодательства, которое так или иначе соприкасается с указанной тематикой, принятие специального нормативного-правового акта будет способствовать комплексному регулированию вопросов обеспечения информационной безопасности, а также устранению недостатков,

создававших правовую неопределенность для участников рассматриваемых отношений в части автоматизированного мониторинга кибербезопасности объектов информационной инфраструктуры, что особенно актуально в контексте поступательного наращивания информационной инфраструктуры во всех сферах жизнедеятельности общества и государства.

Нормативным правовым актом следовало бы предусмотреть использование существующего в действующем законодательстве понятийного аппарата, создание национальной системы обеспечения кибербезопасности, в том числе определить задачи и элементы такой системы.

Обращаем внимание, что принятие такого нормативного правового акта будет способствовать еще и улучшению рейтинга Республики Беларусь в Глобальном индексе кибербезопасности, при составлении которого во внимание принимается наличие законодательства о киберпреступлениях, о борьбе со спамом, а также законодательства, предусматривающего защиту данных, уведомления о нарушениях, онлайн защиту интересов детей, ответственность Интернет-провайдеров и др.