УДК 342

ОБ ОТДЕЛЬНЫХ НАПРАВЛЕНИЯХ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ГОСУДАРСТВЕННЫХ ОРГАНОВ РЕСПУБЛИКИ БЕЛАРУСЬ

И.И. Костян

Национальный центр законодательства и правовых исследований Республики Беларусь,
ул. Берсона 1а, г. Минск, 220030, Беларусь

В условиях стремительного научно-технического прогресса, активной цифровизации белорусского общества, активизации информационного противоборства резко возрастает количество угроз и вызовов в сфере информационной безопасности, в том числе для системы государственных органов, являющейся одним из наиболее уязвимых сегментов в данном контексте. Проведенный в рамках исследования анализ действующего законодательства Республики Беларусь и международных документов позволяет выделить ряд основных направлений по формированию механизма обеспечения информационной безопасности функционирования государственных органов на современном этапе, что в свою очередь создает платформу для нормативного закрепления соответствующих правоотношений.

Ключевые слова: государственные органы, информационная безопасность, цифровизация, информационная общество, киберпреступность.

CERTAIN DIRECTIONS OF ENSURING INFORMATION SECURITY OF STATE BODIES OF THE REPUBLIC OF BELARUS

I.I. Kostyan

Legal Research Institute of the National Center for Legislation and Legal Research of the Republic of Belarus,
1a Bersona street, Minsk, 220030, Belarus

In the conditions of rapid scientific and technological progress, active digitalization of the Belarusian society, activation of information confrontation, the number of threats and challenges in the field of information security is sharply increasing, including one of the most vulnerable segments - the system of state bodies. The analysis of the current legislation of the Republic of Belarus and international documents carried out within the framework of the study allows to identify a number of main directions for the formation of a mechanism for ensuring information security of state bodies at the present stage, which in turn creates a platform for the normative consolidation of relevant legal relations.

Keywords: state bodies, information security, digitalization, information society, cybercrime.

В условиях активной цифровизации белорусского общества, находящегося в авангарде развития сферы информационных технологий, государство должно быть готово к появлению новых угроз в информационном пространстве.

Государственный аппарат, ввиду важности возложенных на него общественных функций, объема концентрируемой там информации является одним из наиболее уязвимых сегментов с точки зрения обеспечения информационной безопасности всего белорусского общества.

Вызовы и угрозы, сопровождающие формирование информационного общества в Республике Беларусь, переопределяют необходимость формирования надежного механизма обеспечения информационной безопасности государственных органов является залогом стабильного развития общества в политической, экономической, социальной и других сферах. Определение основных тенденций в области обеспечения информационной безопасности государственных органов позволят предопределить конкретные меры необходимые для защиты государства от внешних угроз в условиях формирования постиндустриального общества, а также сформировать доктринальную базу для нормативного закрепления информационной безопасности государственного сегмента.

На значимость сферы информационных технологий и важность регламентации происходящих в ней процессов указывает ряд международных и национальных стратегических документов.

В соответствии с ч.1 п.2 Стратегии сотрудничества государств – участников Содружества независимых государств в построении и развитии информационного общества на период до 2025 года, утвержденной Решением Совета глав правительств Содружества независимых государств от 28 октября 2016 г. использование информационно-коммуникационных технологий является одним из приоритетов и необходимым условием повышения качества жизни граждан, развития экономической, социально-политической и культурной сфер жизни общества, а также совершенствования системы государственного управления [1].

Согласно п.п.1, 2 Концепции информационной безопасности Республики Беларусь, утвержденной постановлением Совета Безопасности Республики Беларусь от 18 марта 2019 г. №1 (далее – Концепция) на нынешнем этапе мирового развития информационная сфера приобретает ключевое значение для современного человека, общества, государства и оказывает всеобъемлющее влияние на происходящие экономические, политические и социальные процессы в странах и регионах. Вместе с тем трансформация социума в информационное общество порождает новые риски, вызовы и угрозы, которые напрямую затрагивают вопросы обеспечения национальной безопасности, в том числе защищенность информационного

пространства, информационной инфраструктуры, информационных систем и ресурсов [2]. От правильного понимания таких угроз зависит эффективность механизма обеспечения информационной безопасности государства и общества.

Проблематика угроз информационной безопасности нашла отражение уже в Концепции сотрудничества государств - участников Содружества Независимых Государств в сфере обеспечения информационной безопасности, утвержденной Решением Совета глав государств Содружества Независимых Государств от 10 октября 2008 г., согласно п.4.1 которой угрозы информационной безопасности могут иметь объективный и субъективный характер, выражаться в явлениях, процессах и действиях (или их совокупности), исходить от внешних и внутренних источников [3]. В общих чертах такие угрозы можно поделить на семь ключевых структур, которые задают направления в области обеспечения информационной безопасности государства: нежелательный контент; несанкционированный доступ; утечки информации; потеря данных; мошенничество; кибервойны; кибертерроризм [4, с. 187].

Согласно п.15 Концепции целью обеспечения информационной безопасности является достижение и поддержание такого уровня защищенности информационной сферы, который обеспечивает реализацию национальных интересов Республики Беларусь и ее прогрессивное развитие [2]. Мы солидарны с мнением И. В. Днепровской, что системообразующим элементом модели комплекса национальных интересов по мнению является именно государственная составляющая, так как государство представляет собой центральное организационное, регулирующее и контролирующее учреждение общества [5, с. 30]. При этом, государство – это абстрактное, обезличенное понятие. Оно действует опосредованно через уполномоченные органы государственной власти и должностные лица, которые реализуют его волю [6, с. 97].

Таким образом, именно государственный орган является важнейшим структурным элементом государственного механизма. В процессе осуществления возложенных на них законом полномочий государственные органы непрерывно подвержены всем угрозам, вызванным стремительным развитием информационно-технической сферы, что переопределяет необходимость принятия мер по обеспечению информационной безопасности их функционирования. Анализ положений законодательства позволяет выделить несколько направлений, складывающихся в контексте принятия таких мер.

а) Выявление угроз информационной безопасности. На государственном уровне осуществляются мониторинг, анализ и оценка состояния информационной безопасности, применяются индикаторы оценки ее состояния

(п.16 Концепции) [1]. Именно систематическое изучение окружающего государственные структуры информационного пространства позволяет выделить границы их информационной безопасности.

б) Защита персональных данных и обеспечение конфиденциальности личной информации. Обязанность государства по созданию условий для защиты персональных данных и безопасности личности и общества при их использовании закреплена в ч.2 ст.28 Конституции Республики Беларусь [9]. Государством обеспечивается конституционное право граждан на тайну личной жизни и иную охраняемую законом тайну, защиту персональных данных и авторских прав, а также соблюдение баланса прав с ограничениями, связанными с обеспечением национальной безопасности (п.17 Концепции) [2]. Согласно ч.2 ст.4 Закона Республики Беларусь «О защите персональных данных» от 7 мая 2021 г. №99-З обработка персональных данных должна быть соразмерна заявленным целям их обработки и обеспечивать на всех этапах такой обработки справедливое соотношение интересов всех заинтересованных лиц [10]. Анализ нормативных положений обозначенной тенденции позволяет выделить в ней два направления: 1) обеспечение защиты персональных данных, тайны личной жизни должностных лиц государственных органов, осуществляющих в рамках своей профессиональной деятельности функционал по представлению интересов государства; 2) выделение исключительных ситуаций получения государственными органами в рамках их деятельности личных (конфиденциальных) данных граждан при строгом соблюдении баланса прав граждан и интересов национальной безопасности (в том числе информационной безопасности самого государственного элемента).

в) Контроль за обеспечением безопасности в сфере деятельности средств массовой информации. Формируются правовые, организационные и технологические условия для безопасности функционирования национальных средств массовой информации (далее – СМИ), осуществляется государственный и общественный контроль их деятельности (п.17 Концепции) [2]. Работа государственных органов, всегда привлекает внимание СМИ, и от того, насколько объективно в них отражается деятельность государственных органов, зависит восприятие государства обществом, вырабатывается отношение граждан к власти и их доверие к государственным структурам. Кроме того, в условиях сложной геополитической обстановки на формирование общественного сознания серьезно влияют информационные потоки из вне. Так, в условиях активизации «информационных войн» Законом Республики Беларусь от 24 мая 2021 г. №110-З «Об изменении законов по вопросам средств массовой информации» (далее – Закон №110-З) [11] внесены существенные изменения в Закон Республики Беларусь от 17 июля 2008 г. №427-З «О средствах массовой информации» (далее – Закон о СМИ),

которые выразились в принятии в том числе мер по: минимизации иностранного влияния на средства массовой информации (п. 1.5, 1.6 ст. 15 Закона о СМИ); введению новых ограничений для учредителей средств массовой информации (п. 3.3 ст. 10 Закона о СМИ); дополнению оснований для лишения аккредитации журналистов (п. 2-1 ст. 35 Закона о СМИ); запрету к распространению ряда информации, имеющей деструктивный характер (п.п. 1.4, 1.5 ст.38 Закона о СМИ) и др. [12].

г) Привитие культуры безопасного пользования информационными ресурсами. Повышается осведомленность граждан и общества об угрозах национальной безопасности и государственных мерах по ее обеспечению, их вовлеченность в обеспечение безопасности информационной сферы (п.17 Концепции) [2]. Развитие культуры пользования информационными ресурсами, как профилактика нарушений в данной области, должно осуществляться как путем повышения уровня осведомленности самих работников государственных органов (в том числе технического персонала), так и путем проведения государственными структурами соответствующей разъяснительной работы среди населения.

д) Разработка технических условий информационной безопасности в государственных органах. Государство всесторонне содействует защищенности национальных информационных систем. В целях улучшения устойчивости государственного сектора к информационным рискам осваиваются передовые технологии, внедряются новые средства и способы обеспечения информационной безопасности (п.18 Концепции) [2]. Создаются защищенные системы межведомственного электронного документооборота (абз.8 ч.8 п.4.9 Стратегии) [1]. Наращивается научный потенциал и финансирование работ по исследованию и созданию новых решений в сфере обеспечения информационной безопасности, в том числе технической защиты информации, криптологии, криминологии, криминалистики (п.22 Концепции) [2]. Без технической оснащенности государственных органов не представляется возможным обеспечить соответствие процессов цифровизации государственных структур современному уровню научно-технического прогресса.

е) Совершенствование кадровой политики в сфере информационных технологий. Сегодня уделяется особое внимание кадровому потенциалу в обеспечении информационной безопасности. На современном образовательном и технологичном уровне осуществляется специальная подготовка, переподготовка и повышение профессиональной квалификации лиц, обеспечивающих информационную безопасность, сотрудничество между государственными органами, учреждениями образования и отраслевыми предприятиями в подборе, подготовке и трудоустройстве таких кадров, интегрирование тематики информационной безопасности в образовательные

программы всех уровней обучения. Формируется государственный заказ на подготовку кадров (п.21 Концепции) [2]. Таким образом, технологическому потенциалу государственных органов должен соответствовать надлежащий уровень подготовки работников указанных структур, как специализированных (технических), так и непосредственно, осуществляющих профильный функционал государственного органа. Такой уровень подготовки необходимо поддерживать непрерывным повышением квалификации указанных работников в информационной сфере.

ж) Взаимодействие государства по вопросам информационной безопасности с международным сообществом и общественными институтами. Предпринимаются усилия по повышению действенности международного права и соблюдению моральных норм ответственного поведения в информационном пространстве, оказывается содействие разработке и внедрению мер по укреплению доверия в информационном пространстве. (п.23 Концепции) [2]. В рамках Содружества независимых государств ведется обмен информацией и техническими средствами борьбы с нарушениями против информационной безопасности (абз.11 ч.8 п.4.9 Стратегии) [1]. Развивается взаимодействие государства, общественности, бизнес-сообщества, СМИ в целях своевременного обнаружения рисков и вызовов информационной безопасности, воспрепятствования кибератакам и акциям деструктивного информационного воздействия, повышения эффективности правоохранительной деятельности (п.20 Концепции) [2]. Информационная защищенность государственных органов не должна отождествляться с их изолированностью от всех информационных процессов, в том числе на международном уровне.

е) Регламентация ответственности в сфере информационной безопасности. Деяния, причиняющие существенный вред правоохраняемым интересам в информационной сфере или создающие опасность его причинения, криминализируются в уголовном законе в соответствии с существующими мировыми подходами. Осуществляется выявление и привлечение к установленной законом ответственности лиц, наносящих вред государственным информационным системам, обеспечивается государственная защита интересов граждан и организаций вне зависимости от форм собственности (п.19 Концепции) [2]. Так, глава 23 Кодекса Республики Беларусь об административных правонарушениях (далее – КоАП) предусматривает административную ответственность за совершение административных правонарушений в области связи и информации: несанкционированный доступ к компьютерной информации (ст.23.4 КоАП), нарушение законодательства о защите персональных данных (ст.23.7 КоАП) и др. [13]. Главой 31 Уголовного кодекса Республики Беларусь (далее – УК) регламентирована уголовная ответственность за совершение преступлений против информационной безопасности:

несанкционированный доступ к компьютерной информации (ст.349 УК), уничтожение, блокирование или модификация компьютерной информации (ст.350 УК) и др. [14]. Не меньшее значение для обеспечения безопасного функционирования государственных органов сегодня имеет регламентация гражданско-правовой ответственности в информационной сфере.

Деятельность государственного аппарата, находящегося в эпицентре общественной жизни, нуждается в непрерывном обеспечении информационной безопасности в условиях цифровизации.

Трансформация общественных отношений в современном мире, развивающемся в направлении формирования информационного общества, порождает ряд факторов и явлений, представляющих опасность для функционирования государственных органов.

Принятие государством мер по противостоянию указанным угрозам складывается в ряд тенденций по обеспечению информационной безопасности. Выделение указанных тенденций на основе анализа действующего законодательства Республики Беларусь позволяет выделить ряд основных направлений по формированию механизма обеспечения информационной безопасности функционирования государственных органов на современном этапе, что в свою очередь создает платформу для нормативного закрепления основ информационной безопасности процесса функционирования государственных органов.

Библиографический список

1. Стратегия сотрудничества государств - участников Содружества независимых государств в построении и развитии информационного общества на период до 2025 года [Электронный ресурс] : утв. решением Совета глав правительств Содружества независимых государств от 28 октября 2016 г. // ЭТАЛОН. / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2022.
2. Концепция информационной безопасности Республики Беларусь [Электронный ресурс] : утв. постановлением Совета Безопасности Республики Беларусь, 18 марта 2019 г., №1 // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2022.
3. Концепция сотрудничества государств - участников Содружества Независимых Государств в сфере обеспечения информационной безопасности [Электронный ресурс] : утв. решением Совета глав правительств Содружества независимых государств от 10 октября 2008 г. // ЭТАЛОН. / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2022.
4. Наскидашвили, К. А. Информационная безопасность. Виды угроз информационной безопасности / К. А. Наскидашвили // Вестник студенческого научного общества ГОУ ВПО «Донецкий национальный университете». – 2020. – Т. 1. – № 12. – С. 187–189.
5. Днепровская, И. В. Государственная составляющая в модели комплекса национальных интересов страны / И. В. Днепровская // Современная экономика: проблемы и решения. – 2010. – № 8. – С. 30-39.

6. Романова, В. В. Понятие органа государственной власти / В. В. Романова // Вектор науки Тольятинского государственного университета. – 2009. – № 5(8). – С. 97-99.

7. Марченко, М. Н. Теория государства и права: учебник. – 2-е издание / М.Н. Марченко – М. : Проспект, 2019. – 640 с.

8. О государственной службе [Электронный ресурс] : Закон Респ. Беларусь, от 1 июня 2022 г., №175-З // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2022.

9. Конституция Республики Беларусь [Электронный ресурс] : с изм. и доп., принятыми на респ. референдумах 24 нояб. 1996 г. и 17 окт. 2004 г., в ред. Закона Республики Беларусь от 12 окт. 2021 г. N 124-З, Решения республиканского референдума от 4 марта 2022 г. утв. постановлением Совета Безопасности Республики Беларусь // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2022.

10. О защите персональных данных : Закон Респ. Беларусь, от 7 мая 2021 г., №99-З // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2022.

11. Об изменении законов по вопросам средств массовой информации : Закон Респ. Беларусь, от 24 мая 2021 г., №110-З // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2022.

12. О средствах массовой информации : Закон Респ. Беларусь, от 17 июля 2008 г., №427-З // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2022.

13. Кодекс Республики Беларусь об административных правонарушениях [Электронный ресурс] : 6 января 2021 г., N 91-З, : принят Палатой представителей 18 декабря 2020 г. : одобр. Советом Респ. 18 декабря 2020 г. : в ред. Закона Респ. Беларусь от 04.01.2022 N 144-З // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2022.

14. Уголовный кодекс Республики Беларусь [Электронный ресурс] : 9 июля 1999 г., № 275-З : принят Палатой представителей 2 июня 1999 г. : одобр. Советом Респ. 24 июня 1999 г. : в ред. Закона Респ. Беларусь от 12.05.2022 г. // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2022.