

ПРИОРИТЕТНЫЕ НАПРАВЛЕНИЯ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В РЕСПУБЛИКЕ БЕЛАРУСЬ

О. Г. Шляхтова

*Гомельский государственный университет имени Франциска Скорины,
ул. Советская, 135/60, 246007, г. Гомель, Беларусь, luna116@mail.ru*

Разработка механизмов обеспечения информационной безопасности Республики Беларусь включает в себя мероприятия по информатизации, прежде всего правовой сферы. Первоочередными мероприятиями по реализации государственной политики обеспечения информационной безопасности Республики Беларусь являются разработка и внедрение механизмов реализации правовых норм, регулирующих отношения в информационной среде.

Ключевые слова: информационная безопасность; цифровизация; информационная среда; киберпреступления.

INFORMATION SECURITY PRIORITIES IN THE REPUBLIC OF BELARUS

O. G. Shlyahтова

*Francisk Skorina Gomel State University,
Sovetskaya St., 135/60, 246007, Gomel, Belarus, luna116@mail.ru*

The development of mechanisms for ensuring information security of the Republic of Belarus includes measures for informatization, primarily in the legal sphere. The primary measures for the implementation of the state policy for ensuring information security of the Republic of Belarus are the development and implementation of mechanisms for the implementation of legal norms governing relations in the information environment.

Keywords: information security; digitalization; information environment; cybercrime.

Постепенный процесс становления Республики Беларусь как сильного и процветающего государства невозможно рассматривать без контекста развития новых глобальных тенденций и реалий. Одной из таких реалий является тот факт, что в настоящее время мир находится на этапе перехода от индустриального общества к информационному. Глобальная компьютеризация (цифровизация) с одной стороны открывает перед обществом новые возможности, с другой – стремительное развитие технологий, увеличение количества электронных устройств, услуг и интернет-сервисов привели к появлению рисков и угроз и, в свою очередь, к росту числа кибер-

преступлений. В связи с этим остро встают вопросы обеспечения информационной безопасности.

Основные направления обеспечения информационной безопасности в Республике Беларусь заключаются в нескольких аспектах:

1) Правовой аспект. Информационная безопасность – состояние защищенности сбалансированных интересов личности, общества, государства от внешних и внутренних угроз в информационной сфере [1, п. 8] и является важным приоритетным направлением правового регулирования в Республике Беларусь.

Существует ряд законодательных актов, которые предъявляют требования к обеспечению безопасности различных видов деятельности: Декрет № 8 от 21.12.2017 г. «О развитии цифровой экономики», Стратегия развития информатизации в Республике Беларусь на 2016–2022 гг., Государственная программа развития цифровой экономики и информационного общества на 2021–2025 гг., Концепция информационной безопасности от 18 марта 2019 г. Кроме того, существует ряд других нормативно-правовых актов, которые регулируют вопросы информационной безопасности, в том числе законы о защите окружающей среды и природных ресурсов, о защите государственных секретов, Положение о криптографической защите данных и др. Также постоянно совершенствуются и уголовно-правовые нормы, касающиеся преступлений в информационной среде.

Считаем, что одним из средств повышения уровня цифровой безопасности является дальнейшее укрепление нормативной базы. Назрела необходимость принятия документа стратегического планирования, в котором обеспечение информационной безопасности как составляющей национальной безопасности определено одним из основных долгосрочных приоритетов. Представляет интерес Доктрина информационной безопасности Российской Федерации, утвержденная Указом Президента РФ № 646 от 05.12.2012 г. [2]. Проведя анализ данного нормативного акта, можно отметить, что Доктрина Российской Федерации содержит значительный и емкий комплекс мер, которые направлены на регламентацию общественных отношений в области информационной безопасности. Полагаем, что такой опыт необходимо принять во внимание в процессе подготовки Республикой Беларусь сходного правового акта. Нельзя не учесть и тот факт, что в законодательстве нашей страны действует значительное число норм, предусматривающих ответственность за противоправные деяния в информационной среде, тем самым особо отмечая Беларусь на фоне стран Таможенного союза. Поэтому наш опыт регулирования и регламентации отношений в рассматриваемой сфере, а также

опыт Российской Федерации, необходимо учитывать другими государствами.

Стоит отметить, что первые шаги к созданию единого документа об обеспечении безопасности в цифровой среде уже сделаны. Президент Республики Беларусь 14 февраля 2023 г. подписал Указ «О кибербезопасности». Данный нормативный правовой акт объединяет положения Концепций национальной и информационной безопасности Беларуси и направлен на создание в республике национальной системы обеспечения кибербезопасности.

2) Технический аспект. Обеспечение информационной безопасности является серьезной проблемой для правительств, предприятий и частных лиц. Согласно Глобальному индексу кибербезопасности (GCI), который представляет собой глобальное исследование, проводимое Международным союзом электросвязи (МСЭ), в 2020 г. Беларусь заняла 97-е место из 194 стран с точки зрения уровня кибербезопасности [3]. С 2017 г. рейтинг нашей страны по данному исследованию падает: 2017 г. – 39-е место, 2018 г. – 69-е место, 2019 г. – 89-е место. Снижение происходило не за счет ослабления по оцениваемым параметрам, а благодаря усилению позиций других государств. Все это позволяет говорить о том, что страны все больше уделяют внимание уровню своей кибербезопасности и достигают определенного прогресса в ответ на новые вызовы. В блоке стран СНГ Беларусь стабильно занимает 5-е место с 2017 г. GCI учитывает такие факторы, как нормативно-правовая база, технические меры, организационные меры, меры в отношении сотрудничества и наращивание потенциала.

В Беларуси, как и во многих других странах, необходимость защиты конфиденциальной информации от несанкционированного доступа, кражи или неправомерного использования становится все более важной по мере развития технологий и передачи и хранения большего количества информации в цифровом виде. Органы государственного управления в информационной сфере обеспечивают технические возможности доступа к информационным ресурсам для всех категорий пользователей, формируют государственные информационные ресурсы путем создания эффективной сети сбора и накопления информации, системы стандартизации, сертификации и контроля качества информационных продуктов и сетей, предпринимают меры к созданию единой развитой системы классификации и кодирования информации.

3) Организационный аспект. Стоит отметить, что, как и многие другие страны, Беларусь, сталкивается с рядом проблем в области информационной безопасности, в том числе с необходимостью соблюдения ба-

ланса безопасности и конфиденциальности, быстрыми темпами технологических инноваций и растущим числом киберугроз.

В Республике Беларусь принимается ряд мер по совершенствованию своих технических мер и наращиванию потенциала в области информационной безопасности. Создана система сертификации специалистов по информационной безопасности, которая позволяет отдельным лицам пройти сертификацию в различных областях кибербезопасности. Правительство обеспечивает обучение и сертификацию специалистов через Национальный центр электронных услуг. Стоит отметить, что данный центр является оператором важнейших межведомственных информационных систем, составляющих основу электронного правительства. Беларусь сохраняет свои позиции с высоким уровнем готовности к электронному правительству и входит в топ-40 стран по уровню развития технологий, что стало возможным благодаря госпрограммам по цифровизации.

Помимо существующей нормативно-правовой базы органы государственного управления осуществляет ряд других мероприятий для обеспечения информационной безопасности. Например, в стране реализован ряд технических мер по защите информации, включая использование шифрования, межсетевых экранов и систем обнаружения вторжений.

Важным направлением является также раскрытие новейших тенденций в области международного сотрудничества по вопросу обеспечения информационной безопасности. Республика Беларусь является государством-участником стран СНГ и принимает участие в обсуждении вопросов, связанных с сотрудничеством в области информационной безопасности, реализуемым в рамках международных организаций, функционированием и развитием безопасного Интернет-пространства, а также с межведомственным взаимодействием.

Республика Беларусь также является государством-наблюдателем Шанхайской организации сотрудничества (ШОС), которая создала Региональную антитеррористическую структуру (РАТС), осуществляющая борьбу и с кибертерроризмом.

Республика Беларусь инвестирует в исследования и разработки в области кибербезопасности, включая разработку новых технологий и инструментов для защиты информации. Например, в Оперативно-аналитическом центре при Президенте Республики Беларусь (ОАЦ) будет создан Национальный центр кибербезопасности (НЦК). Правовая основа создания и функционирования национальной системы обеспечения кибербезопасности определена Указом Президента Республики Беларусь от 14.02.2023 г. № 40 «О кибербезопасности».

В целом эти и другие меры демонстрируют приверженность Беларуси к совершенствованию своих технических мер, наращиванию потенци-

ала в области информационной безопасности, которая является приоритетным направлением.

4) Социальный аспект. В Беларуси с каждым годом растет количество пользователей сети Интернет. Однако уровень цифровой грамотности все еще остается низким. Интернет является источником информации в различных сферах для большинства пользователей и занимает лидирующие позиции в информационном пространстве, отодвинув телевидение на второе место [4]. В связи с этим целесообразно для повышения уровня цифровой грамотности граждан проводить семинары, тренинги, брифинги, курсы по повышению квалификации работников, создавать службы информационной безопасности в организациях и на предприятиях. В учреждениях образования проводить единые дни информирования детей и молодежи, ввести в учебные программы дисциплины или специальные курсы, позволяющие изучать основы цифровой безопасности.

Растущая информатизация общества усилила влияние информационной составляющей в системе национальной безопасности Республики Беларусь, что объективно требует эффективного функционирования системы информационно-психологического обеспечения национальной безопасности страны.

Следует иметь в виду, что при возникновении конфликтных ситуаций и усилении степени противостояния государств с различными идеологиями и культурами «информационная борьба», которая практически постоянно ведется в мирное время, легко может перерасти в агрессивную «информационную войну». Вмешательство во внутренние дела государств, нарушение суверенитета и культуры народов, разжигание недоверия и вражды между народами – это прямая политическая и психологическая подготовка к реальной войне, а также экономической дестабилизации и манипулированию информацией со стороны противника, как в мирное, так и в военное время.

Исходя из этого, необходимо предпринимать меры по защите психики населения, социальных групп, граждан от деструктивных информационно-психологических воздействий общественного мнения, противодействовать попыткам манипулирования процессами восприятия информации населением со стороны враждебных Республике Беларусь политических сил, проводимых с целью ослабления политической стабильности и обороноспособности государства, отстаивать национальные интересы, цели и ценности Беларуси в информационном пространстве (европейском, стран СНГ, национальном).

Стоит отметить, что МВД проводится активная информационная и правовая работа по снижению деструктивного влияния экстремистских Интернет-ресурсов на сознание белорусского населения, недопущению

реабилитации нацизма, введению ответственности по отдельным статьям административного и уголовного законодательства.

В соответствии с постановлением Совета Министров от 12.10.2021 г. № 575 «О мерах противодействия экстремизму и реабилитации нацизма» регламентирована работа по признанию экстремистскими формированиями и привлечению к уголовной ответственности их создателей и активных участников. По данным МВД, на сегодня таковыми признаны более 300 Telegram-каналов и чатов [5, с. 6].

В 2021–2022 гг. по заявлениям МВД информационная продукция 778 Telegram-каналов (чатов) и иных Интернет-ресурсов признана судами экстремистскими материалами.

В результате идеологической, информационной, нормотворческой и практической работы органов внутренних дел по снижению деструктивного влияния экстремистских Интернет-ресурсов с осени 2021 г. по настоящее время зафиксировано более 500 тыс. отписок пользователей от основных экстремистских Telegram-каналов и чатов (всего их более 1 тыс., а количество подписчиков более 2 млн.), специализировавшихся на белорусской повестке.

В условиях возрастающего информационного давления на Республику Беларусь приоритетной задачей для редакций государственных СМИ является создание качественного и аргументированного контрпропагандистского контента. В эфире всех теле- и радиоканалов Белтелерадиокомпании, а также в сообществах в социальных сетях оперативно размещается информация официальных представителей государственных органов и организаций, связанная с реагированием на распространение фейков и вбросов деструктивной информации.

Телеканал «ОНТ» запустил проект «Антифейк», созданы спецрубрики (например, «Будет дополнено»), реализуются авторские проекты «Полит STAND UP», «Пропаганда». На телеканале «СТВ» опровержение фейковых новостей осуществляется в информационно-аналитической программе «Неделя». Активно работают БелТА, «СБ. Беларусь сегодня», «Звезда», другие центральные издания. Большая работа в данном направлении ведется региональными СМИ. Созданы специальные рубрики, проекты (в том числе в соцсетях): «Факты против фейков», «Развеиваем слухи», «Достоверно», «Актуально», «Стоп! Фейк!», «Антифейк», «Острый ракурс», «По слухам» и др. [5, с. 7].

Таким образом, Республика Беларусь является динамично развивающейся страной, где год от года в разные сферы деятельности внедряются новые информационные технологии, увеличивается количество цифровых услуг и т.д. Цифровая трансформация страны требует одновременно совершенствования экономических и правовых аспектов, регули-

рующих сферу информационных технологий. Существует необходимость закрепления на законодательном уровне акта, который будет основой для формирования государственной политики и развития общественных отношений в области обеспечения информационной безопасности, а также для выработки мер по совершенствованию системы безопасности в информационной сфере. Наличие фундаментальной и четко регламентированной нормативно-правовой базы наиболее полно обеспечит защиту законных интересов общества и государства от угроз в информационной среде.

В то же время необходимо постоянно привлекать инвестиции, развивать технологии и оборудование, повышать цифровую грамотность населения. Важны образовательные меры, обеспечивающие повышение осведомленности людей об информационных угрозах. Они должны предусматривать разработку и внедрение образовательных курсов по информационной безопасности, о безопасном поведении в сети. Целесообразно также расширение каналов обратной связи для информирования о подозрительных, заведомо ложных и экстремистских сообщениях в информационном пространстве.

Можно сделать вывод, что национальная безопасность Республики Беларусь во многом будет зависеть от эффективности обеспечения её информационной безопасности.

Библиографические ссылки

1. О Концепции информационной безопасности Республики Беларусь [Электронный ресурс] : постановление Совета Безопасности Республики Беларусь, 18 марта 2019 г. № 1. Режим доступа: <https://etalonline.by/document/?regnum=p219s0001>. Дата доступа : 28.10.2022.

2. Об утверждении Доктрины информационной безопасности Российской Федерации [Электронный ресурс] : Указ Президента РФ, 5 декабря 2016 г., № 646. Режим доступа: <https://www.garant.ru/products/ipo/prime/doc/71456224/>. Дата доступа : 11.02.2023.

3. Глобальный индекс кибербезопасности 2020 г. [Электронный ресурс]. Режим доступа : <https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTML-E>. Дата доступа : 01.07.2023.

4. Председатель Президиума НАН Беларуси – об информационной безопасности страны [Электронный ресурс]. Режим доступа: <https://pravo.by/novosti/obshchestvenno-politicheskie-i-v-oblasti-prava/2019/mart/33256/>. Дата доступа : 02.07.2023.

5. Основные направления государственной политики в области информационной безопасности : материалы для членов информационно-пропагандистских групп (декабрь 2022 г.) / Академия управления при Президенте Республики Беларусь. Минск, 2022. С. 10.