Концепция информационной безопасности Республики Беларусь – взгляд в будущее

Владимир АРЧАКОВ, заместитель Государственного секретаря Совета Безопасности Республики Беларусь, генерал-майор

Олег МАКАРОВ, директор Белорусского института стратегических исследований, доктор юридических наук, доцент

Алексей БАНЬКОВСКИЙ, начальник информационно-аналитического управления Государственного секретариата Совета Безопасности Республики Беларусь, кандидат юридических наук

Вследствие новизны отношений, возникающих в информационной сфере, она подвержена повышенной уязвимости к рискам, вызовам и угрозам, которые в свою очередь транспортируются во все иные сферы общественной жизни, а проблема обеспечения информационной безопасности становится важнейшим вопросом реализации сбалансированных интересов личности, общества и государства. Обеспечение информационной безопасности превращается в самостоятельную область жизнедеятельности общества, а поэтому требует комплексного, системного подхода на основе общепринятых взглядов и принципов. В данной статье авторы и разработчики Концепции информационной безопасности дополнительно раскрывают ее значение с точки зрения теоретического и практического применения.

Национальная Концепция информационной безопасности (далее – Концепция) утверждена 18 марта 2019 года *[1]*. Данный документ разработан с участием различных государственных органов и организаций, а также ведущих представителей отечественного экспертного сообщества, ученых и специалистов, а его основные положения апробированы на различных международных конференциях. В силу избранного обществом пути цивилизационного развития информационная сфера в последние десятилетия приобрела новые свойства отдельной области общественной жизни. Произошедшие изменения не просто линейное разрастание информационной сферы, а ее качественное преобразование. Значимость информационных отношений, а также скорость их трансформации в особую информационную экосистему определяют необходимость осмысления новых условий существования социума.

Необходимость конкретизации в национальных правовых и иных обще-

◀ Встреча Государственного секретаря Совета Безопасности Республики Беларусь С.В. Зася с научно-экспертной группой. 2018 год

ственных отношениях информационной безопасности как обособленного феномена и нормативного института объективно продиктована формированием и довольно динамичным дальнейшим развитием в нашей стране информационного общества *[2]*. В то же время указанная в Концепции основная обобщающая категория «информационная безопасность» была закреплена только в Уголовном кодексе Республики Беларусь, фактически подменяя более узкое понятие «компьютерная безопасность», а также в законах, ратифицирующих международные соглашения Беларуси с Россией (Соглашение между Правительством Республики Беларусь и Правительством Российской Федерации о сотрудничестве в области обеспечения международной информационной безопасности от 25 декабря 2013 года) и государствами – участниками СНГ в области обеспечения международной информационной безопасности (Соглашение о сотрудничестве государств – участников Содружества Независимых Государств в области обеспечения информационной безопасности от 20 ноября 2013 года; модельный закон МПА СНГ «Об информации, информатизации и информационной безопасности» от 28 января 2014 года № 41-15; и др.), международных актах (Соглашение о сотрудничестве государств – членов Организации Договора о коллективной безопасности в области обеспечения информационной безопасности от 30 ноября 2017 года; Положение о сотрудничестве государств – членов ОДКБ в сфере обеспечения информационной безопасности от 10 декабря 2010 года; Протокол о взаимодействии государств – членов ОДКБ по противодействию преступной деятельности в информационной сфере от 23 декабря 2014 года, ратифицированный Законом Республики Беларусь от 15 июля 2015 года № 292-З; и др.). Понятийный аппарат, рассредоточенный в различных отраслях права и нормативных правовых актах, был и пока остается сложным и противоречивым. При наличии значительного количества локальных правовых предписаний в информационной сфере незадекларированными оставались базовые правовые подходы к обеспечению информационной безопасности. В целом в государстве и обществе становилась все более очевидной потребность в преодолении весьма разрозненного представления о состоянии защищенности информационной сферы. Исходя из этого, необходимость разработки Концепции вызвана новыми условиями безопасности общества, потребностью осознания сущности и особенностей их развития, важностью определения направлений и последовательности действий по обеспечению информационной безопасности.

В первую очередь в Концепции определяются цели и задачи обеспечения ин-

формационной безопасности в нынешних условиях социально-экономического развития Республики Беларусь. Предметом концептуального рассмотрения выступают именно стратегические цели и приоритеты в области обеспечения информационной безопасности, а также сущность и содержание необходимых мер. Обстоятельно разъясняются цели и направления государственной политики обеспечения безопасности информационной сферы, основанные на соблюдении сбалансированных интересов личности, общества и государства.

Впервые вводится понятие «информационный суверенитет» как неотъемлемое и исключительное верховенство права Республики Беларусь самостоятельно определять правила владения, пользования и распоряжения национальными информационными ресурсами, осуществлять независимую внешнюю и внутреннюю государственную информационную политику, формировать национальную информационную инфраструктуру, обеспечивать информационную безопасность. Его достижение предполагается обеспечивать в том числе на основе нового принципа «информационного нейтралитета», предусматривающего проведение миролюбивой внешней информационной политики, уважение общепризнанных и общепринятых прав любого государства в данной сфере, исключение инициативы вмешательства в информационную сферу других стран.

Концепцией четко разделяются гуманитарный и технологический аспекты состояния и развития информационной сферы, а следовательно, и конкретные объекты (предметы) обеспечения информационной безопасности. С учетом того, что в основополагающей Концепции национальной безопасности и документах, связанных с ее реализацией, эти объекты в общем нашли свое отражение, теперь получило развитие понимание вызовов, угроз, степени их опасности, форм и методов противодействия. Фактически сформулирована более отчетливая государственная политика по защите национальных интересов в информационной сфере, включающая также и реагирование на риски, вызовы и угрозы. Определяются три конкретных объекта обеспечения информационной безопасности – информационно-психологическая компонента информационной сферы (массовое сознание), информационная инфраструктура и информационные ресурсы (включая государственные секреты). Причем ключевым является понимание того, что информационная безопасность, в том числе реагирование на риски и вызовы в информационной сфере, должна обеспечиваться не просто всеми государственными органами, тем более не только правоохранительным блоком, а взаимосвязанными, взаимодополняющими и всеобъемлющими действиями государства, общества и граждан.

При рассмотрении вышеуказанных объектов информационной безопасности существенное внимание уделено безопасности информационно-психологической компоненты информационной сферы. Распространение запрещенного, недостоверного, негативного контента в информационном пространстве отрицательно влияет на население, обусловливает риски девальвации жизнесберегающих ценностей и традиционных нравственных ориентиров, снижение темпов образовательного и духовного развития, размывание национальной идентичности, деградацию личности. Информационно-психологическими воздействиями может провоцироваться конфликтная поляризация белорусского общественного сознания, политическая, религиозная, этническая нетерпимость, неудовлетворенность общественным устройством, состоянием окружающей среды. Снижается порог критического восприятия информации, повышается «доверчивость» общества.

Анализ зарубежного опыта показывает, что через информационное пространство фактически происходит вмешательство во внутренние дела государства, преднамеренная дискредитация его конституционных основ, побуждение к гражданскому неповиновению. Информационно-психологическое воздействие составляет сущность таких

современных угроз, как гибридные, информационные, сетецентрические войны, «цветные революции», и, следовательно, необходимо концентрировать усилия государства на нейтрализации подобного воздействия всеми возможными способами. Безусловно, это выдвигает отчетливые требования эффективно противостоять возникающим рискам, вызовам и угрозам в информационном пространстве, прогнозировать и адекватно реагировать на наиболее острые и организованные информационные акции по деформации общественного сознания и снижению уровня национальной безопасности в целом.

Так, необходимо постоянное исследование обстановки в информационном пространстве. Ее мониторинг следует проводить с высокой степенью интенсивности, объективно, на современном технологическом уровне, и об этом прямо говорится в Концепции. Предупреждение деструктивного информационно-психологического воздействия на население должно осуществляться главным образом за счет активной, наступательной и скоординированной информационной деятельности всех государственных структур, а не только и не столько путем ограничения информационных потоков и фрагментарного реагирования на какие-либо информационные поводы. Небезынтересно в связи с этим привести прозвучавшее мнение главного редактора радиостанции «Эхо Москвы» А. Венедиктова о том, что «Александр Лукашенко правильно поставил диагноз тех угроз, которые на нас идут. В условиях цифровой революции, социальных сетей каждый человек, не имеющий отношения к журналистике и СМИ, имеет возможность создавать собственный информационный поток. И если мы не будем противостоять этой волне, не возглавим ее своим именем, она нас просто захлестнет» *[3]*.

Немаловажно, что в принятых концептуальных подходах указывается на необходимость государственно-правовой поддержки национальных СМИ. Тенденция неуклонного увеличения в телевизионном эфире количества высокорейтинговых зарубежных каналов обусловливает заметный отток аудитории от государственного телевидения, снижение популярности государственных телеканалов, утрату ими позиций на внутреннем рекламном рынке и снижение потенциала развития. Тогда как известно, что в России, иных постсоветских государствах и странах Запада на законодательном уровне обеспечивается эффективная защита собственного информационного пространства, активно практикуются такие меры, как установление предельного соотношения количества отечественных и зарубежных программ, достаточно жесткое ограничение иностранного аудиовизуального продукта, ограничение (в том числе квотирование и полное исключение) иностранных телеканалов, из числа имеющих право размещать рекламу и др.

Отдельного и весьма пристального внимания требует активное и эффективное присутствие государства в интернете, который на сегодня является одним из главных источников информации для массовой аудитории и наиболее действенным инструментом информационно-психологического влияния на общественное сознание. Несмотря на то, что электронные ресурсы и интернет-сервисы становятся основным источником новостной информации, государственные органы зачастую пренебрегают информационной деятельностью в глобальной сети.

Конечно, определенные меры, направленные на наведение порядка в информационном пространстве, принимаются. Например, внесение в 2018 году соответствующих изменений в Закон Республики Беларусь «О средствах массовой информации» от 17 июля 2008 года № 427-З. Однако законодательство в этой быстро трансформирующейся сфере должно совершенствоваться с учетом развития как общественных отношений, самих СМИ, так и технологий деструктивных информационных воздействий. Причем это совершенствование не будет чрезмерно резким. Во-первых, подходы разных государств к обеспечению безопасности в сфере смыслов существенно различаются.

Готовой, универсальной для всех матрицы мер не выработано, и Беларусь руководствуется собственным постепенным пониманием ее возможной конструкции. Во-вторых, в общественном сознании пока нет четкого понимания того, какие цели преследует государство при наведении этого порядка, чем они диктуются, каким образом будут достигаться в дальнейшем и к чему надо быть объективно и детерминированно готовым в плане правового регулирования и ограничений.

Концепция нацеливается на формирование такого понимания. В ней эти проблемы описываются в их современном понимании, а безопасность информационного пространства в качестве источника формирования массового сознания прямо определена одним из важнейших условий развития нашего государства с его традиционными, конституционно закрепленными ценностями. При этом четко обозначаются главные приоритеты деятельности по обеспечению защищенности сферы смыслов: это сохранение традиционных устоев и ценностей, информационное обеспечение и сопровождение государственной политики, безопасность массовой информации. Одновременно закладываются важные посылы об обеспечении более комфортных условий национальным СМИ, о повышении их конкурентоспособности, активизации присутствия государства в интернете.

Что касается обеспечения защищенности национальной информационной инфраструктуры, в Концепции получила правовое осмысление такая очевидная стратегическая проблема и новая область отношений, как кибербезопасность. Данное понятие уже устойчиво закрепилось в мировом официальном лексиконе, да и Республика Беларусь без каких-либо препятствий участвует в глобальных и иных «кибериниициативах» (межгосударственные рейтинги, резолюции ООН, международные конференции и т. п.). Причем главное – не просто определиться в понятиях, а обеспечить их практическую реализацию конкретными исполнителями, сопряженность с международными подходами и неуклонное следование страны в общемировом русле, тем более что Беларусь объективно не может быть «законодателем мод» в данном вопросе.

Немаловажно и то, что проблема кибербезопасности в условиях глобальных противоречий постоянно обостряется. Всевозможные кибервоздействия становятся предметом международных дискуссий и разногласий, используются в мире как средство устрашения и политического шантажа, рассматриваются как повод для санкций. В некоторых государствах проведение кибероперациий предусматривается в доктринальных и стратегических документах национального уровня, а в вооруженных силах создаются и развиваются кибервойска. Все это требует максимального понимания самой сущности кибербезопасности, достичь которого исключительно через свои «собственные» определения (а тем более при их отсутствии) было бы невозможно.

Наряду с этим обеспечение кибербезопасности связано с вполне осязаемыми на сегодня рисками и вызовами, и действия государства по их выявлению и локализации должны быть не только активными и последовательными, но определенными и закрепленными на перспективу. Причем эти риски и вызовы уже оказывают негативное влияние на состояние национальной безопасности. Фиксируются попытки несанкционированного доступа к информационным системам государственных органов и организаций, внедрения в информационную инфраструктуру вредоносного программного обеспечения. Увеличивается количество правонарушений и преступлений с использованием информационно-коммуникационных технологий (ИКТ). Усложняются процессы и технологии, требующие все более высокой квалификации работников. Пока не складывается общего понимания необходимости особой защиты критически важных объектов информатизации (КВОИ), и поэтому не вполне срабатывают соответствующие нормативные и организационные меры. Сохраняется высокая зависимость Республики Беларусь от импорта информационных техноло-

гий, средств информатизации и защиты информации, продолжается использование несертифицированных импортных программно-технических средств. Утрачивается национальный научный потенциал. Знания и представления о современных угрозах информационной инфраструктуре в обобщенном виде не обновляются и не ложатся в основу объективно обусловленных контрмер.

С учетом этого в Концепции вводится понятие кибербезопасности и ее производных, конкретизируются направления и меры защиты национального сегмента сети интернет, КВОИ, государственных информационных систем, борьбы с киберпреступностью.

Вопросы безопасности информационных ресурсов также нуждались в объединении общим концептуальным замыслом. Причем тема их защищенности в общем контексте информационной безопасности намного шире, нежели безопасность компьютерной информации. Для выстраивания последовательной государственной политики в этой области устанавливается всеобъемлющая связь между общедоступной информацией, государственными информационными ресурсами, информацией ограниченного распространения всевозможных видов, персональными данными граждан. На основании этого в каждом из данных сегментов выделяются главенствующие приоритеты (баланс свободы информации и права на тайну, гарантированность государством распространения или предоставления общедоступной информации, безопасный доступ к информационным ресурсам добросовестных пользователей, целесообразность и соразмерность реализации защитных мер).

В Концепции Беларусь позиционируется как страна, максимально вовлеченная в мировые информационные процессы, приверженная лучшим мировым и международным практикам обеспечения информбезопасности, демонстрируется приемлемость различных норм и стандартов. Наряду с очевидным и объективным превалированием в Концепции собственных национальных подходов к

проблемам информационной безопасности, соблюдением духа и буквы международных актов, заключенных в этой сфере нашей страной, в ней также упоминаются тематические резолюции Генассамблеи ООН («Использование информационно-коммуникационных технологий в целях развития», 2011; «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности», 2018; и др.), рекомендации ОБСЕ *[4; 5]* (причем в Концепции фактически имплементированы отдельные положения документов в сфере борьбы с кибертерроризмом, такие как решение «Консолидированная концептуальная база ОБСЕ для борьбы с терроризмом», 2012, и др.), некоторые конкретные европейские концепты, отдельные тезисы из иных общемировых документов *[6; 7; 8; 9; 10]*.

Кроме того, в ней говорится о наших конкретных приверженностях, которые можно четко соотносить с так называемыми моделями международной информационной безопасности. На экспертном уровне таких моделей выделяют две, условно называя их «евро-атлантической» и «евразийской». В первой из них информационно-психологическая (контентная) составляющая умалчивается, а обеспечение информационной безопасности трактуется только как противодействие киберпреступности. Вторая модель, и ее придерживается несоизмеримо большее число государств, в том числе Беларусь, говорит в целом об ответственном и доб-

росовестном поведении государств в информационной сфере.

Надо сказать и о том, что с принятием своей Концепции у нашей страны появится дополнительный и вполне весомый повод не только для более активного участия в определении, а если понадобится – и в установлении необходимых правил поведения в информационном пространстве, но и для выдвижения собственных инициатив. Причем в ближайшем будущем, видимо, не следует рассчитывать на общее глобальное понимание и согласование правовых норм в сфере информационной безопасности. В этих условиях Республике Беларусь необходимо целенаправленно и последовательно выстраивать жизнеспособную систему международной информационной безопасности вокруг себя, в том числе на основе собственных и узнаваемых общих авторитетных принципов.

Необходимость стройных концептуальных взглядов обусловливается и потребностью в постоянном развитии законодательства. При общей урегулированности информационных отношений в Республике Беларусь систему нормативного обеспечения информационной безопасности можно охарактеризовать как не совсем целостную. Каждый законодательный акт в области информатизации, средств массовой информации или связи содержит только отдельные элементы правового регулирования безопасности без выделения специальных субъектов и особых мер («своими силами»). Остаются и конкретные неурегулированные вопросы, причем во многих случаях не вполне ясно, какие векторы следует задавать новым нормативным установкам. Например, потребуется дальнейшая правовая регламентация использования сети интернет, включающего интересы реализации государственной политики в коммуникационной среде, архитектуру общественного взаимодействия, обеспечение прав и интересов всех субъектов отношений, в том числе законодательное закрепление государственной деятельности по воспрепятствованию деструктивным информационно-психологическим воздействиям. Необходима дополнительная правовая поддержка национальным СМИ. Не исключено, что придет время воспользоваться зарубежной практикой о введении правовых запретов на распространение информации, прямо посягающей на основополагающие идейные государственные ценности (в странах Балтии запрещается пропагандировать коммунизм, в Германии – нацизм, в Украине – советскую символику, в России – реабилитировать нацизм и т. д.).

Следует также продолжить совершенствование подходов к обеспечению безопасности КВОИ, защите государственных секретов, служебной информации ограниченного распространения, персональных данных. Возможно, уже в ближайшее время станет целесообразной криминализация кибертерроризма, использования ИКТ для совершения преступлений против половой неприкосновенности несовершеннолетних (т. н. груминг детей), распространения фейковой информации, повлекшей за собой материальный или моральный ущерб, использования ботнетов для совершения преступлений, осуществления незаконных сделок с криптовалютами.

Вообще юридические нормы в информационной сфере, в том числе в области информатизации и информационной безопасности, уже образуют самостоятельную отрасль права в Республике Беларусь. Однако в силу недостаточной сформированности философско-ценностной платформы пока не просматривается общая и устойчивая структура этой отрасли, которая позволяла бы динамично, без ошибок, повторов и пробелов создавать национальное законодательство на основе общих выработанных взглядов. Как представляется, принятие концептуальных установок будет во многом способствовать решению и этой задачи.

Анализируя значение принятия Концепции, нельзя не учитывать, что на сегодняшний день практически все развитые государства, в том числе сопредельные с Республикой Беларусь, располагают собственными доктринальными документами в области информационной безопасности. Это объясняется

вышеупомянутой новизной рисков, вызовов, угроз для возникающих общественных отношений и объективной невозможностью решить «все и сразу» на законодательном уровне.

Таким образом, принятие Концепции позволяет:

– обеспечить дальнейшее формирование системы официальных взглядов на проблему информационной безопасности на современном этапе развития общества;

– закрепить основные направления, формы и методы обеспечения информационной безопасности, развивать их и дополнять по мере генерирования новых знаний и технологий;

– обстоятельно информировать общество о проблемах обеспечения информационной безопасности, обоснованности и обусловленности государственной политики в этой сфере, а также обеспечить доведение до международного сообщества обобщенных взглядов Республики Беларусь на эти проблемы в прогрессивном ключе;

– консолидировать усилия государства и общества, направленные на повышение эффективности защиты национальных интересов в информационной сфере в условиях глобальной информатизации и возникновения новых угроз информационной безопасности;

– обеспечить целенаправленную и неуклонную интеграцию Беларуси в системы обеспечения международной информационной безопасности на основе национальных приоритетов.

Положения Концепции соответствуют потребностям и возможностям общества и государства, так как они непосредственно связаны с общенациональными установками V Всебелорусского народного собрания, на котором одним из факторов устойчивого развития Беларуси на ближайшую пятилетку определено дальнейшее внедрение информационных технологий во все сферы жизнедеятельности общества *[11]*. Понятия, суждения, оценки и предлагаемые в Концепции механизмы обеспечения информационной безопасности соответствуют положениям Конституции, основываются на Концепции национальной безопасности, иных нормативных правовых актах Республики Беларусь, программных документах национального развития, научных исследованиях и подходах.

Принятие Концепции информационной безопасности не требует срочного и обязательного внесения изменений в действующее законодательство. В то же время ее положения послужат основой для дальнейшего нормотворчества в информационной сфере. Разработанная система концептуальных взглядов может учитываться при подготовке иных документов стратегического планирования, государственных программ, разработке соглашений в области международной информационной безопасности.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. О Концепции информационной безопасности [Электронный ресурс]: Постановление Совета Безопасности Республики Беларусь, 18 марта 2019 г., № 1 // Официальный Интернет-портал Президента Республики Беларусь. – Режим доступа: http://president.gov.by/uploads/documents/2019/1post.pdf. – Дата доступа: 19.03.2019.

2. Об утверждении Концепции национальной безопасности Республики Беларусь [Электронный ресурс]: Указ Президента Респ. Беларусь, 9 окт. 2010 г., № 575 // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2019.

3. Лукашенко правильно поставил диагноз стоящих перед СМИ угроз – Венедиктов [Электронный ресурс] // Белорусское телеграфное агентство. – 2017. – 12 июля. – Режим доступа: https://www.belta.by/society/view/lukashenko-pravilno-postavil-diagnoz-stojaschih-pered-smi-ugroz-venediktov-256969-2017/. – Дата доступа: 25.02.2019.

4. Борьба с использованием Интернета в террористических целях [Электронный ресурс]: Решение Совета Министров ОБСЕ, № 3/04 (MC.DEC/3/04/Corr.I), 7 декабря 2004 г. – Режим доступа: https://www.osce.org/ru/resources/csce-osce-key-documents /. – Дата доступа: 25.02.2019.

5. Противодействие использованию Интернета в террористических целях [Электронный ресурс]: Решение Совета Министров ОБСЕ, № 7/06 (MC.DEC/7/06/Corr.I), 5 декабря 2006 г. – Режим доступа: https://www.osce.org/ru/resources/csce-osce-key-documents /. – Дата доступа: 25.02.2019.

6. Консолидированная концептуальная база ОБСЕ для борьбы с терроризмом [Электронный ресурс]: решение № 1063, 7 декабря 2012 г. – Режим доступа: https://www.osce.org/ru/resources/csce-osce-key-documents /. – Дата доступа: 25.02.2019.

7. Конвенция о защите физических лиц при автоматизированной обработке персональных данных [Электронный ресурс]. – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_121499/. – Дата доступа: 25.02.2019.

8. Общий регламент по защите данных ЕС, 27 апреля 2016 г. [Электронный ресурс]. – Режим доступа: https://eugdpr.org/. – Дата доступа: 25.02.2019.

9. Глобальная программа кибербезопасности Международного союза электросвязи (подраздел 19. Обусловленность мер) [Электронный ресурс]. – Режим доступа: https://www.itu.int/en/action/cybersecurity/Pages/gca.aspx. – Дата доступа: 04.02.2019.

10. Доклад группы правительственных экспертов ООН по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности (2015) [Электронный ресурс]. – Режим доступа: https://www.un.org/disarmament/ru/. – Дата доступа: 25.02.2019.

11. Ключевая задача на пятилетие – устойчивый экономический рост [Электронный ресурс]: резолюция V Всебелорусского собрания // Белорусское телеграфное агентство. – 2016. – 23 июня. – Режим доступа: http://shod.belta.by/news-ru/view/kljuchevaja-zadacha-na-pjatiletie-ustojchivyj-ekonomicheskij-rost-rezoljutsija-vsebelorusskogo-195859-2016/. – Дата доступа: 25.02.2019.