Мировое значение информационной сферы

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. В результате повышения насыщенности и динамики общественных отношений, мировых и региональных событий, роста всеобщего интеллектуального потенциала значительно увеличиваются информационные потребности людей.

Формируемое в глобальном масштабе информационное общество представляет собой новый этап развития цивилизации с преобладанием знаний и информации, воздействием информационных технологий на все сферы человеческой деятельности. Кардинально повышается роль информационных технологий в реализации прав и свобод граждан.

Индустрия телекоммуникации стала одной из наиболее динамичных и перспективных сфер мировой экономики. С процессами информатизации все больше связываются национальные экономические интересы и перспективы инвестиций.

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.

Актуальность и значение Концепции информационной безопасности Республики Беларусь

Формирование в Республике Беларусь информационного общества, обеспечивающего доступность информации, распространение и использование знаний для поступательного и прогрессивного развития, рассматривается как национальный приоритет и общегосударственная задача. В связи с этим актуальность и значение Концепции информационной безопасности Республики Беларусь (далее – Концепция) обуславливаются следующими факторами:

повышением значимости формирования информационного общества в Республике Беларусь, его роли в социально-экономическом развитии Беларуси как суверенного и независимого государства, безопасности реализации национальных стратегий и планов создания цифровой экономики и научно-технического прогресса в целом;

необходимостью предметной и всесторонне осознанной защиты национальных интересов в информационной сфере, определяемых Концепцией национальной безопасности Республики Беларусь, обобщения практически и научно обоснованных взглядов на обеспечение

информационной безопасности, конкретизации и детализации подходов к данной деятельности;

необходимостью рассмотрения информационной безопасности как обособленного феномена и нормативного института, а также правового закрепления основ государственной политики по защите национальных интересов в информационной сфере;

формированием новой сферы общественных отношений по обеспечению информационной безопасности;

важностью улучшения координации и управляемости деятельностью субъектов, вовлеченных в развитие информационной сферы и обеспечение ее безопасности, устойчивого и последовательного функционирования механизмов реагирования на риски, вызовы и угрозы информационной безопасности;

необходимостью информирования граждан, а также международного сообщества о принятых в Республике Беларусь взглядах на сферу информационной безопасности и приоритетах ее обеспечения;

интеграцией Беларуси в систему международной информационной безопасности, важностью повышения концептуальной и технологической совместимости и синхронизации целей и задач национальной системы обеспечения информационной безопасности с корреспондирующими системами других государств и организаций.

Основные понятия и определения

Для целей настоящей Концепции используются следующие понятия и их определения:

воздействие на информацию – действие по изменению формы предоставления и/или содержания информации;

государственная информационная система – совокупность банков данных, информационных технологий и комплекса (комплексов) программно-технических средств, формируемая или приобретаемая за счет средств республиканского или местных бюджетов, государственных внебюджетных фондов, а также средств государственных юридических лиц;

государственный информационный ресурс – организованная совокупность документированной информации, включающая базы данных, другие совокупности взаимосвязанной информации в информационных системах, формируемая или приобретаемая за счет средств республиканского или местных бюджетов, государственных внебюджетных фондов, а также средств государственных юридических лиц;

деструктивное информационное воздействие – осуществление информационного влияния на политические и социально-экономические

процессы, деятельность государственных органов, а также на физических и юридических лиц в целях ослабления обороноспособности государства, нарушения общественной безопасности, принятия и заключения заведомо невыгодных решений и международных договоров, ухудшения отношений с другими государствами, создания социально-политической напряженности, формирования угрозы возникновения чрезвычайных ситуаций, разрушения традиционных духовных и нравственных ценностей, создания препятствий для нормальной деятельности государственных органов, а также причинения иного ущерба национальной безопасности;

защита информации – комплекс правовых, организационных и технических мер, направленных на обеспечение конфиденциальности, целостности, подлинности, доступности и сохранности информации;

информационная безопасность – состояние защищенности сбалансированных интересов личности, общества и государства от внешних и внутренних угроз в информационной сфере;

информационная инфраструктура – совокупность технических средств, систем и технологий создания, преобразования, передачи, использования и хранения информации;

информационный суверенитет Республики Беларусь – неотъемлемое и исключительное верховенство права государства 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;

информационная сфера – совокупность информации, информационной инфраструктуры, субъектов, осуществляющих сбор, формирование, распространение и использование информации, а также системы регулирования возникающих при этом общественных отношений;

информационное пространство – область деятельности, связанная с созданием, преобразованием, передачей, использованием, хранением информации, оказывающая воздействие в том числе на индивидуальное и общественное сознание и собственно информацию;

кибератака – целенаправленное воздействие программных и (или) программно-аппаратных средств на объекты информационной инфраструктуры, сети электросвязи, используемые для организации взаимодействия таких объектов, в целях нарушения и (или) прекращения их функционирования и (или) создания угрозы безопасности обрабатываемой такими объектами информации;

кибербезопасность – состояние защищенности информационной инфраструктуры и содержащейся в ней информации от внешних и внутренних угроз;

киберинцидент – событие, которое фактически или потенциально угрожает конфиденциальности, целостности, подлинности, доступности и сохранности информации, а также представляет собой нарушение (угрозу нарушения) политик безопасности;

кибертерроризм – атаки на информационные системы, несущие угрозу здоровью и жизни людей, а также способные спровоцировать серьезные нарушения функционирования критически важных объектов в целях оказания воздействия на принятие решений органами власти, либо воспрепятствования политической или иной общественной деятельности, либо устрашения населения, либо дестабилизации общественного порядка;

киберустойчивость – способность информационной системы предвидеть и своевременно адаптироваться к изменениям обстановки в целях успешного предотвращения негативных последствий или быстрого восстановления после киберинцидента;

международная информационная безопасность – состояние международных отношений, исключающее нарушение мировой стабильности и создание угрозы безопасности государств и мирового сообщества в информационном пространстве;

обеспечение информационной безопасности – система мер правового, организационно-технического и организационно-экономического характера по выявлению угроз информационной безопасности, предотвращению их реализации, пресечению и ликвидации последствий реализации таких угроз;

преступления в информационной сфере – предусмотренные уголовным законом преступления против информационной безопасности (киберпреступления) и иные преступления, предметом или средством совершения которых являются информация, информационные системы и сети;

суверенитет данных – подчиненность отношений по поводу информации в цифровой форме, возникающих на территории Беларуси, национальной юрисдикции Республики Беларусь.

Иные термины в Концепции приведены в значениях, используемых в законодательстве Республики Беларусь и международных актах, участницей которых является Республика Беларусь.

РАЗДЕЛ II
СОСТОЯНИЕ И РАЗВИТИЕ ИНФОРМАЦИОННОЙ СФЕРЫ В РЕСПУБЛИКЕ БЕЛАРУСЬ

Гуманитарный аспект

Основополагающим национальным интересом Республики Беларусь в информационной сфере с точки зрения гуманитарного аспекта является реализация конституционных прав граждан на получение, хранение и распространение полной, достоверной и своевременной информации, свободу мнений, убеждений и их свободного выражения, а также права на тайну личной жизни.

В настоящее время состояние информационной сферы в Республике Беларусь характеризуется высоким уровнем доступа населения страны к массовой информации. Количество национальных средств массовой информации (СМИ) и интернет-ресурсов неуклонно увеличивается, формируется при участии государства и в негосударственном секторе. Белорусское информационное пространство открыто для активной работы иностранных СМИ и интернет-ресурсов. В стране ежегодно увеличивается пропускная способность внешних каналов доступа в сеть Интернет, количество интернет-пользователей, абонентов сетей электросвязи. Также развивается информационное взаимодействие граждан, создаются сетевые сообщества для коммуникации, обмена информацией, опытом и знаниями, общественного обсуждения проектов нормативных правовых актов, широко применяется практика краудфайндинга, повышается роль общественных советов и независимых экспертов в принятии решений государственными органами, формируются институты общественного самоконтроля в целях сохранения исторического, культурного наследия и укрепления правосознания.

В целом белорусскому информационному пространству в полной мере свойственны мировые тренды информатизации, в том числе перевод СМИ в цифровой формат (дигитализация), сочетание их различных типов (мультимедийность), адаптация информационного продукта к распространению через Интернет, сближение и слияние в нем различных типов СМИ (конвергенция).

В то же время мировое развитие информационно-коммуникационных технологий (далее – ИКТ) обуславливает постоянное появление новых источников информации, что объективно снижает в информационном пространстве долю отечественного контента и требует более активной работы по его продвижению. Исходя из этого необходимо на государственном уровне предпринимать меры по повышению объема, разнообразия и качества национального контента, скорости его предоставления, доверия населения к официальной информации и государственным СМИ, адаптации форм распространения информации

к первоочередным информационным потребностям граждан, а также достижению баланса интересов личности, общества и государства.

Технологический аспект

Основными направлениями информатизации в Республике Беларусь определены развитие эффективной и прозрачной системы государственного управления, обеспечение быстрых, удобных и безопасных коммуникаций между государством, бизнесом и гражданами, модернизация национальной информационной инфраструктуры, внедрение ИКТ в реальном секторе экономики, совершенствование социальной сферы на основе ИКТ, укрепление собственной отрасли информационных технологий.

Цифровая трансформация экономики является важнейшей составляющей формирования информационного общества и одним из главных направлений развития Республики Беларусь, в результате которого в ближайшие десятилетия все отрасли, рынки, сферы жизнедеятельности государства должны быть переориентированы на новые цифровые экономические модели. Для решения этой задачи в стране определены структура управления информатизацией и архитектура электронного правительства. Развиваются инновационные цифровые технологии, основанные на системах искусственного интеллекта, нейронных сетей, обеспечивающие работу с разнообразными информационными ресурсами, в том числе массивами больших данных, методах распределенных вычислений (облачные технологии), технологии реестра блоков транзакций (блокчейн).

Беларусь последовательно участвует в процессах информатизации на трансграничном контуре, в том числе в рамках Союзного государства Беларуси и России, Евразийского экономического союза, Содружества Независимых Государств, Европейского союза и иных мировых систем политического и экономического взаимодействия и партнерства.

Наряду с этим, объем применения информационных технологий в реальном секторе экономики остается невысоким. Степень цифровизации отраслей экономики различна, что снижает ожидаемый синергетический эффект от синхронной информатизации, и с учетом этого следует разрабатывать цифровую политику для конкретных сфер государственной жизнедеятельности, ориентировать пилотные проекты цифровизации на их отраслевое масштабирование, создавать центры компетенции по вопросам цифровой трансформации. Требуется переход электронного правительства от простого предоставления услуг по запросам граждан к проактивной работе с населением. Быстрое развитие ИКТ и увеличение информационных потребностей общества обуславливают необходимость

освоения новых стандартов в сфере телекоммуникаций, повышения производительности и надежности сетевой инфраструктуры.

Состояние информатизации и в целом информационной сферы в Республике Беларусь характеризуется общепринятыми в мире аналитическими отчетами и международными рейтингами, в том числе лежащими в основе показателей социально-экономического развития государства и обеспечения национальной безопасности.

РАЗДЕЛ III
ГОСУДАРСТВЕННАЯ ПОЛИТИКА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Цели и направления государственной политики

Целью обеспечения информационной безопасности является достижение и поддержание такого уровня защищенности информационной сферы, который обеспечивает реализацию национальных интересов Республики Беларусь и ее устойчивое развитие.

Обеспечение информационной безопасности осуществляется в соответствии с государственной политикой в данной области, которая включает в себя формирование, совершенствование и реализацию организационных, правовых, научно-технических, правоохранительных, экономических мер обеспечения национальной безопасности в информационной сфере. В свою очередь, именно через развитие этой сферы главным образом обеспечивается и ее безопасность.

На государственном уровне осуществляется мониторинг, анализ и оценка состояния информационной безопасности, применяются индикаторы оценки ее состояния. Определяются приоритетные направления предотвращения угроз информационной безопасности, минимизации их деструктивного воздействия и локализации последствий. Разрабатывается и реализуется комплекс мер стратегического и тактического характера по предупреждению и нейтрализации информационных рисков, вызовов и угроз.

Обеспечивается конституционное право граждан свободно искать, получать, передавать, производить и распространять информацию любым законным способом, право 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. Формируются правовые, организационные и технологические условия для безопасности функционирования национальных средств массовой информации, а также осуществляется государственный и общественный контроль их деятельности. Реализуется

максимальная доступность для граждан и организаций государственных электронных услуг, административных процедур и информационных ресурсов государственных органов и организаций. Повышается осведомленность граждан и общества об угрозах национальной безопасности и государственных мерах по ее обеспечению, их вовлеченность в обеспечение безопасности информационной сферы.

Государство всесторонне содействует защищенности национальных информационных систем, обеспечению безопасности используемого гражданами и организациями программного обеспечения. В целях улучшения устойчивости государственного сектора к информационным рискам осваиваются передовые технологии, внедряются новые средства и способы обеспечения информационной безопасности. Разрабатываются стандарты информационной безопасности и с их учетом проводится аудит государственных систем информационной безопасности. Развивается смарт-проектирование решений по обеспечению информационной безопасности. На нормативном уровне выделяется и регламентируется функционирование критически важных объектов информатизации (КВОИ). Поощряется развитие технологий безопасности в бизнесе и жизнедеятельности граждан.

Деяния, причиняющие существенный вред правоохраняемым интересам в информационной сфере или создающие опасность его причинения, криминализируются в уголовном законе в соответствии с существующими мировыми подходами. Реализуются шаги по снижению угроз киберпреступности, в том числе кибертерроризма, расследованию и пресечению действий вовлеченных в террористическую деятельность лиц, перекрытию каналов пропаганды терроризма, привлечения и вербовки сторонников, поощрения и провоцирования террористической активности, финансирования терроризма. Вводятся правовые режимы безопасности информации и информационных ресурсов, технические условия и политики безопасности. Осуществляется выявление и привлечение к установленной законом ответственности лиц, наносящих вред государственным информационным системам, обеспечивается государственная защита интересов граждан.

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.

Осуществляется 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. 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.

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. Создаются и развиваются каналы международного обмена опытом в области обеспечения информационной безопасности, а также информацией об угрозах национальным интересам, в том числе уязвимостях информационных систем, инцидентах в информационной инфраструктуре.

Государство осуществляет финансирование приоритетных направлений обеспечения информационной безопасности, прежде всего в рамках государственных программ. Формируется государственный заказ на подготовку кадров, производятся средства обеспечения информационной безопасности, разрабатываются инновационные методы и технологии защиты информационных ресурсов и систем.

Информационный суверенитет

В условиях обострения международных противоречий становится проблематичным выработать эффективные и общепринятые правила поведения мирового сообщества в информационном пространстве. Подходы различных стран к оценке угроз в информационной сфере и противодействию им не совпадают, а по отдельным направлениям поляризируются.

В связи с этим важнейшей целевой установкой обеспечения информационной безопасности является информационный суверенитет Республики Беларусь.

Информационный суверенитет достигается, прежде всего, путем формирования системы правового регулирования отношений в информационной сфере, обеспечивающей безопасное устойчивое развитие, социальную справедливость и согласие.

В рамках данной системы государство обеспечивает развитие национальных СМИ и телекоммуникаций, современных ИКТ, национальной индустрии производства средств информатизации, а также защиту национальных рынков информационных и телекоммуникационных услуг, снижающих зависимость от технологий иностранного производства и сокращающих цифровое неравенство. В обществе воспитывается

и стимулируется критическое отношение к проявлениям неуважения национальных устоев, традиций и нарушениям норм морали и права в информационной сфере, нетерпимость к дезинформации, информационным манипуляциям и иным неявным информационно-психологическим воздействиям.

Формируются правовые условия и границы деятельности зарубежных и международных субъектов в национальном информационном пространстве для обеспечения потребностей граждан во внешнем информационном обмене без культурной и информационной экспансии, вмешательства во внутренние дела Республики Беларусь.

Создаются необходимые условия для построения и безопасного развития функциональной, технологически самодостаточной, надежной и устойчивой информационной инфраструктуры. Осуществляется защита информационных ресурсов, в том числе государственных секретов, иной охраняемой информации, персональных данных, обеспечивающая политическую самостоятельность государства, защищенность жизненного пространства человека, сохранение духовных и культурных ценностей белорусского общества, научно-технологические преимущества и реализацию иных национальных интересов. Республикой Беларусь реализуется принцип ”суверенитета данных“.

Стремление к информационному суверенитету не расходится с международно-правовыми принципами обеспечения прав и свобод, гарантирующих конкурентное и свободное развитие в условиях мировой цифровой трансформации.

Информационный нейтралитет

В международных отношениях информационный суверенитет Республики Беларусь обеспечивается в том числе на основе 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, направленного на дискредитацию или оспаривание их политических, экономических, социальных и духовных стандартов и приоритетов, а также нанесения вреда информационной инфраструктуре каких бы то ни было государств и участия в их информационном противостоянии. При этом Республика Беларусь отстаивает собственные национальные интересы в информационной сфере с использованием всех имеющихся сил и средств.

В целях обеспечения политики информационного нейтралитета повышается степень присутствия Беларуси в мировом информационном пространстве, расширяется международный информационный обмен,

поддерживается установление и регулирование всеобщих правил поведения в данной сфере и осуществляется заключение соглашений по обеспечению международной информационной безопасности.

Государственное реагирование на риски, вызовы и угрозы в информационной сфере

Государство осуществляет реагирование на риски и вызовы в информационной сфере с целью предупреждения их трансформации в угрозы национальной безопасности, развития и масштабирования вредоносного воздействия. Обеспечивает своевременное принятие мер безопасности, незамедлительно оповещает заинтересованных субъектов, минимизирует ущерб и локализует последствия, определяет причастных лиц и организации, накапливает опыт противодействия угрозам.

Государственное реагирование на риски, вызовы и угрозы в информационной сфере предполагает сбор информации об используемых технологиях, способах деструктивных информационных воздействий и совершения киберпреступлений, анализ, оценку и прогнозирование состояния безопасности данной сферы, выявление реализующихся вызовов и угроз, локализацию негативных последствий и восстановление нанесенного вреда (ущерба). Определяется защищенность и устойчивость объектов информационной безопасности, в том числе информационной инфраструктуры, информационных ресурсов, индивидуального, группового и массового сознания к действию угроз. Выявляются и исключаются условия возникновения и реализации рисков, вызовов и угроз информационной безопасности.

Подготавливаются и внедряются сценарии и планы кризисного реагирования на кибератаки, компьютерные инциденты, акты деструктивного информационного воздействия, иные угрозы информационной безопасности, а также проводятся учения и тренировки сил реагирования.

Реализуется политика информационного сдерживания, выражающаяся в демонстрации достоверной готовности к отражению деструктивных информационных воздействий, достаточной возможности технологического, организационного, правового противодействия угрозам в информационной сфере и выявления их источников.

В случае существенного осложнения информационной обстановки, связанного в том числе с необходимостью обеспечения военной безопасности государства, осуществляются дополнительные меры защиты информационной сферы правовыми, информационно-технологическими, техническими и иными методами (информационное противоборство), обеспечивается приоритетное взаимодействие военной организации государства и гражданского сектора.

Кроме того, Вооруженные Силы Республики Беларусь, иные воинские формирования предпринимают меры по обеспечению информационной безопасности в рамках решения возложенных задач по своему непосредственному предназначению с применением современных, высокотехнологичных сил и средств.

Беларусь участвует в международном реагировании на потенциальные риски, вызовы и угрозы информационной безопасности в рамках заключенных договоров и соглашений, осуществляет межгосударственное взаимодействие в анализе рисков, вызовов и угроз информационной безопасности, обмен опытом и совместные практические мероприятия.

РАЗДЕЛ IV
БЕЗОПАСНОСТЬ ИНФОРМАЦИОННОГО ПРОСТРАНСТВА КАК ОДНО ИЗ ВАЖНЕЙШИХ УСЛОВИЙ РАЗВИТИЯ СУВЕРЕННОГО, ДЕМОКРАТИЧЕСКОГО СОЦИАЛЬНОГО ГОСУДАРСТВА

Обусловленность мер

Глобальное возрастание роли информации в системе общественных отношений, открытость информационного пространства и повышение уровня информатизации населения обуславливают новые меры безопасности информационной сферы с точки зрения обеспечения государством полноценной реализации своих суверенных прав и интересов социально-экономического развития.

Механизмы деструктивного информационно-психологического воздействия на личность, общество и государство постоянно совершенствуются, а масштабное манипулирование массовым сознанием принимает такую же остроту, как борьба за территории, ресурсы и рынки. Через информационное пространство осуществляется преднамеренная дискредитация конституционных основ государств и их властных структур, размывание национального менталитета и самобытности, вовлечение людей в экстремистскую и террористическую деятельность, разжигание межнациональной и межконфессиональной вражды, формирование радикального и протестного потенциала. Информационный фактор играет все более значительную роль в межгосударственных конфликтах и неявных действиях, направленных на нарушение суверенитета, территориальной целостности стран и снижение темпов их развития. В результате информационных воздействий существенно меняются социальные связи человека в обществе, стиль мышления, способы общения, восприятие действительности и самооценка.

Все большее беспокойство вызывает активное распространение в информационном пространстве фальсифицированной, недостоверной и запрещенной информации. Снижение критического отношения потребителей информации к ”фейковым“ сообщениям новостных ресурсов, в социальных сетях и на других онлайн-платформах создает предпосылки преднамеренного использования дезинформации для дестабилизации общественного сознания в политических, социально-опасных, иных подобных целях.

В связи с этим особое значение приобретает ответственное поведение всех участников информационных процессов, а также выработка общих правил коммуникации в информационном пространстве, основанных на признании идентичности прав и обязанностей в существующей реальности (физическом мире) и виртуальном пространстве.

Основные направления обеспечения

Для Республики Беларусь основными источниками угроз информационно-психологического характера в информационной сфере являются информационное противоборство между ведущими мировыми центрами силы, целенаправленное формирование внутри и за пределами страны информационных поводов для дискредитации государственной внешней и внутренней политики.

С учетом этого главная цель обеспечения безопасности информационно-психологической компоненты информационной сферы состоит в сохранении информационного суверенитета и проведении политики информационного нейтралитета, а также формировании устойчивого иммунитета против деструктивных информационно-психологических воздействий на массовое общественное сознание, а в необходимых случаях – и противодействие им.

Для этого главным образом необходимо на государственном уровне обеспечивать формирование, использование и развитие информационного пространства исключительно в целях социального, экономического и культурного развития, а также обеспечить постоянную, активную и эффективную деятельность государственных органов, организаций, научно-экспертного сообщества в информационном пространстве, особенно наращивать ее в глобальной сети Интернет.

В приоритетном порядке необходимо поддерживать сохранение в обществе традиционных социальных устоев и ценностей, открытое и всестороннее информационное обеспечение и сопровождение государственной политики, а также воспрепятствование в законном порядке распространению незаконной и недостоверной массовой информации.

Сохранение традиционных устоев и ценностей

Для повышения устойчивости общества к деструктивным информационным воздействиям необходимо сосредоточить усилия на сохранении сформированных в общественном сознании традиционных фундаментальных ценностей народа, выступающих в качестве одного из основных элементов обеспечения его единства и одним из условий неуклонного развития государства.

Информационная политика Республики Беларусь нацеливается на продвижение таких жизненных приоритетов, как гуманизм, миролюбие, добрососедство, справедливость, взаимопомощь, крепкие семейные отношения, здоровый образ жизни, созидательный труд, принятые в белорусском обществе нормы морали и нравственности, позитивное правосознание. В информационной сфере в полной мере находят отражение равные права всех без исключения национальностей, населяющих Республику Беларусь, уважительное отношение ко всем традиционным религиям и вероисповеданиям. Важнейшее значение имеет поддержка и всемерное развитие гражданско-патриотической идеологии.

Белорусский язык, наряду с конституционно закрепленным в государстве двуязычием, содействует повышению национального самосознания белорусского общества и формированию его духовности. Расширение социальных функций и коммуникативных возможностей белорусского языка, его полноценное и всестороннее развитие вместе с другими элементами национальной культуры выступают гарантом гуманитарной безопасности государства.

Требует дальнейшей последовательной реализации государственная историческая политика, направленная на закрепление в Беларуси и за ее пределами белорусской национальной концепции исторического прошлого страны и белорусской модели памяти, построенной в соответствии с этой концепцией в качестве доминирующей.

РАЗДЕЛ V
ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

Обусловленность мер

Цифровая трансформация экономики и инновации в области ИКТ наряду с мировым развитием и наращиванием технологических возможностей во взаимодействии людей, бизнеса, государственных институтов обуславливают необходимость принятия особых мер, обеспечивающих доверие и безопасность при создании и использовании

в современном информационном обществе информационной инфраструктуры и данных в информационных системах.

Политическая и социально-экономическая сферы, общественная и военная безопасность становятся все более уязвимыми перед преднамеренными или случайными технологическими воздействиями, формирующимися в том числе в условиях недостаточных глобальных механизмов согласованного и действенного предупреждения и сдерживания киберинцидентов в сети Интернет.

Повсеместное функционирование объектов промышленности, транспорта, энергетики, электросвязи, здравоохранения и систем жизнеобеспечения с автоматизированными системами управления ставит в прямую зависимость жизнь и здоровье населения, экологическую и социальную безопасность от их надежности и защищенности. Кибератаки на информационную инфраструктуру рассматриваются в мире как одна из наиболее значимых угроз безопасности.

Во многих национальных вооруженных силах создаются и развиваются кибервойска, а проведение кибероперации предусматривается в доктринальных и стратегических документах. Одновременно рассматривается возможность реагирования на кибератаки как на вооруженную агрессию, что в условиях практической невозможности точной идентификации их источников (инициаторов) может привести к бездоказательной и произвольной трактовке обоснованности встречных военных действий.

Неуклонно растет количество киберпреступлений. Информационные системы и ресурсы становятся как предметом преступлений, так и средством их совершения. Формируется тотальная зависимость финансового сектора и иных секторов от надежности электронных систем хранения, обработки и обмена данными.

Однако ни в глобальном, ни в региональных масштабах пока не удается эффективно воспрепятствовать разработкам и распространению средств, заведомо предназначенных для уничтожения, блокирования, модификации, похищения информации в сетях и ресурсах или нейтрализации мер по ее защите. Выработка правовых, процедурных, технических и организационных мер против кибервоздействий на информационные ресурсы отстает от формирования реальных и потенциальных угроз их осуществления.

Основные направления обеспечения

В качестве наиболее вероятных источников угроз кибербезопасности рассматриваются отказы технических средств и сбои программного обеспечения в информационных и телекоммуникационных системах, противоправная деятельность отдельных лиц и преступных групп,

преднамеренные действия и ошибки персонала информационных систем, выражающиеся в нарушении установленных регламентов их эксплуатации и правил обработки информации, зависимость Беларуси от других стран-производителей программных и аппаратных средств при создании и развитии информационной инфраструктуры.

Перед Республикой Беларусь стоит стратегическая цель развития системы обеспечения кибербезопасности, базирующейся на передовых международных подходах управления рисками и предназначенной для реализации долгосрочных мер по их сокращению до приемлемого уровня.

Национальная система обеспечения кибербезопасности должна реализовывать весь возможный комплекс правовых, организационных и технических мер по обеспечению безопасности национальной информационной инфраструктуры, в том числе информационных систем, обеспечивать конфиденциальность, доступность и целостность информации, а также легко трансформироваться и адаптироваться в изменяющейся обстановке за счет постоянного анализа на предмет соответствия актуальным рискам кибербезопасности.

В первую очередь необходимо обеспечить киберустойчивость национального сегмента сети Интернет, критически важных объектов информатизации и государственных информационных систем, эффективное противодействие киберпреступлениям.

Противодействие киберпреступности

В Республике Беларусь создана система предупреждения, выявления, пресечения и всестороннего расследования киберпреступлений. Обеспечивается соответствие норм уголовного закона в данной области уровню общественного развития, мировым тенденциям правового регулирования и передовому зарубежному опыту.

В связи с появлением новых общественно опасных деяний в информационной сфере устанавливается уголовная и иная ответственность за их совершение. Обеспечивается постоянное совершенствование форм и методов предупреждения, выявления, пресечения и расследования киберпреступлений, повышается своевременность и качество оперативно-розыскной деятельности.

Беларусь заинтересована в сближении и унификации подходов противодействия киберпреступлениям на международном уровне, выработке общих стандартов в правоприменительной практике, международном обмене опытом и практическом взаимодействии. Осуществляются реализация регионального и международного сотрудничества в сфере кибербезопасности, отслеживание деятельности

преступных групп и отдельных преступников, действующих в киберпространстве.

Важное значение в противодействии киберпреступлениям имеет повышение доверия между правоохранительными органами, компаниями и предприятиями государственного и частного секторов, образовательными и научными организациями, объединение их усилий в предупреждении, выявлении, пресечении и расследовании киберпреступлений. Одной из эффективных мер предупреждения и профилактики киберпреступлений является снижение мотивации их совершения за счет устранения условий формирования противоправных схем.

Наряду с этим одним из приоритетных направлений деятельности уполномоченных государственных органов является профилактика киберпреступности, основанная на популяризации среди населения, прежде всего молодежи, нетерпимости к асоциальному поведению в информационном пространстве, проведении разъяснительной работы в СМИ и сети Интернет с целью формирования безопасной национальной информационной экосистемы. Для повышения правосознания и снижения уязвимости от кибератак проводится обучение граждан основам поведения в информационной сфере.

РАЗДЕЛ VI
ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ РЕСУРСОВ

Обусловленность мер

Появление широких и доступных возможностей для сбора, хранения и обработки большого объема данных, создание технологий прямого доступа к информации обуславливают необходимость рассматривать ее как самостоятельный и ценный ресурс. Информационные ресурсы становятся приоритетным объектом преступлений и киберинцидентов, подвергаются похищению, модификации, уничтожению, блокированию и другим воздействиям.

Повышается значение технической защиты информации ограниченного распространения, в то время как средства похищения, незаконного блокирования и иного воздействия на информационные ресурсы универсально применяются в политических, военных, разведывательных, экономических, преступных и иных целях.

Множественные угрозы и риски незаконного и необоснованного вмешательства в частную жизнь граждан, похищение персональных данных, компрометация реквизитов доступа и избыточное

профилирование сужает личное пространство человека и нарушает его приватность. Раскрытие личной информации стало неотъемлемым атрибутом корыстных преступлений и преступлений против личности.

Формируется нелегальный рынок баз и банков данных, спрос на которые обуславливает похищение информационных массивов, сопровождаемое нарушением авторских прав.

Основные направления обеспечения

Основными источниками угроз в области обеспечения безопасности информационных ресурсов в Республике Беларусь следует рассматривать деятельность отдельных лиц, преступных групп, недобросовестных отечественных и иностранных организаций, объединений или сообществ, направленную на получение неправомерного доступа к этим ресурсам в политических, военных, коммерческих, личных и иных целях, осуществляемого в обход установленного порядка или вопреки общепринятым нормам морали и нравственности, а также нарушение функционирования информационной инфраструктуры.

Основной целью государственной политики в области обеспечения безопасности информационных ресурсов является сохранение их доступности, целостности и конфиденциальности.

Система обеспечения безопасности информационных ресурсов основана на стратегическом принципе соблюдения баланса свободы информации и права на тайну, гарантиях государства на распространение или предоставление общедоступной информации. Государство обеспечивает расширение безопасного доступа к информационным ресурсам добросовестных пользователей, развитие сервисов качественного и удобного предоставления информации, совершенствование систем ее данных.

На данном этапе необходимо главным образом обеспечивать надежную и всесторонне обусловленную защиту информации ограниченного распространения, безопасность персональных данных и государственных информационных ресурсов.

Защита персональных данных

Достижение защищенности персональных данных обеспечивает взвешенная государственная политика по определению требований к всевозможным субъектам информационных отношений, осуществляющим сбор, обработку и хранение этих данных.

Внимание государства сосредотачивается на совершенствовании нормативной правовой базы в данной области. Государственное

регулирование сбора, обработки, предоставления и распространения персональных данных осуществляется с учетом современного международного опыта, в том числе согласуется с положениями межгосударственных актов (108 Конвенция Совета Европы, GDPR). Формируемые в Беларуси подходы к защите персональных данных базируются на принципе ”безопасность по умолчанию“.

Важной мерой по усилению контроля в этой сфере является функционирование в государстве уполномоченного субъекта (субъектов) по защите прав физических лиц при обработке их персональных данных.

Обеспечение безопасности государственных информационных ресурсов и общедоступной информации

Государство обеспечивает защиту информационных ресурсов, находящихся в распоряжении государственных органов и организаций, а также осуществляет правовое регулирование пользования, владения и распоряжения информационными ресурсами. В этих целях создается единая система учета и сохранности информационных ресурсов, а также применяются специальные процедуры государственной регистрации.

Государственными органами осуществляется защита общедоступной информации от противоправного уничтожения, модификации, блокирования правомерного доступа, необоснованного засекречивания, сокрытия, несвоевременного распространения или предоставления. Государство обеспечивает запрет цензуры, гарантирует оперативное доведение общедоступной информации установленными законодательством способами, расширяет возможности соответствующих сервисов, реализует концепцию ”открытых данных“. Государство заинтересовано в поддержании баланса между потребностью граждан в ознакомлении с общедоступной информацией, их права на отказ от получения такой информации, а также необходимостью ее защиты от противоправных посягательств.

РАЗДЕЛ VII
ГОСУДАРСТВЕННО-ЧАСТНОЕ ПАРТНЕРСТВО В ОБЕСПЕЧЕНИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Эффективному решению задач в обеспечении информационной безопасности должно способствовать постоянное целенаправленное взаимодействие между государственным сектором и коммерческими организациями в форме государственно-частного партнерства с целью привлечения компетенций, кадров, технологий, капитала частных предприятий, повышения отдачи использования бюджетных средств

и активов предприятий, совместной разработки и реализации инвестиционных и иных проектов в области информационной безопасности.

Государственно-частное партнерство в области обеспечения информационной безопасности рассматривается как юридически оформленное сотрудничество государственного органа и субъекта хозяйственной деятельности негосударственной формы собственности или физического лица, основанное на объединении ресурсов и распределении рисков, реализуемое для обеспечения информационной безопасности с привлечением частных инвестиций и компетенций.

Одним из важнейших направлений реализации государственно-частного партнерства в сфере обеспечения информационной безопасности является поддержка отечественных производителей программного обеспечения информационных систем и систем информационной безопасности.

Наряду с преодолением зависимости Беларуси от других стран-производителей программных и аппаратных средств реализация инфраструктурных проектов и проектов, напрямую связанных с обеспечением информационной безопасности через механизм партнерства государства и отечественных частных компаний, должна способствовать формированию рыночного спроса на импортозамещающую национальную информационно-технологическую продукцию, повышению ее качества.

Государство заинтересовано во взаимодействии с IT-компаниями, интернет-провайдерами, операторами связи и внешними экспертами в обновлении и развитии механизмов выявления угроз информационной безопасности через IT-аудит, мониторинг киберрисков, поиск уязвимостей и актуальных средств защиты, выработку правил поведения в Интернете.

Государственно-частное партнерство способствует подготовке квалифицированных кадров в области информационной безопасности, формированию актуальных программ подготовки соответствующих специалистов, внедрению новых образовательных и профессиональных стандартов в данной сфере, а также повышению общей компьютерной грамотности населения, включая обучение людей старшего и среднего возраста компьютерным навыкам, правилам пользования персональными данными, умению безопасной работы в сети Интернет.

В связи с трансформацией общественных отношений в информационной сфере государственно-частное партнерство становится наиболее эффективной моделью обеспечения информационной безопасности. В ней государство определяет цели, стратегические задачи и регулятивные подходы, а бизнес-сообщество предоставляет технологии, знания и ресурсы для решения поставленных задач. При этом государство

стремится гарантировать технологическую нейтральность и защиту частных организаций (и их инвестиций) от возможных рисков.

РАЗДЕЛ VIII
УЧАСТИЕ В ОБЕСПЕЧЕНИИ МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Целью обеспечения международной информационной безопасности является выявление, предупреждение и нейтрализация внешних рисков, вызовов и угроз информационной безопасности.

В рамках обеспечения международной информационной безопасности осуществляется активное, всестороннее, взаимовыгодное международное, в том числе межведомственное, сотрудничество.

Международное сотрудничество в сфере информационной безопасности на региональном, двустороннем, многостороннем и глобальном уровнях направлено на снижение риска использования информационных и коммуникационных технологий для осуществления враждебных действий и актов агрессии в отношении Беларуси.

Обеспечивается участие Беларуси в международных организациях, профильных международных договорах, двусторонних отношениях с иными государствами, в других формах межгосударственного сотрудничества с целью формирования механизмов международного взаимодействия по противодействию угрозам международной информационной безопасности.

Главным средством для достижения целей обеспечения международной информационной безопасности является поддержка и продвижение соответствующих инициатив, отвечающих национальным интересам Республики Беларусь в информационной сфере.

Республика Беларусь поддерживает продвижение мер доверия в сфере международной информационной безопасности и выступает за ответственное поведение государств в информационной сфере, которое предусматривало бы в первую очередь предотвращение в ней конфликтов, а не их урегулирование. Государства должны воздерживаться от целенаправленных деструктивных информационных воздействий на другие страны, исключать использование своей территории для осуществления кибератак, а также противодействовать использованию скрытых вредоносных функций и программных уязвимостей в программно-аппаратных средствах, добиваясь их безопасности для пользователей.

Беларусь принимает участие в международном информационном обмене на основе международных договоров и соглашений, в рамках юрисдикции обеспечивает его безопасность.