О проекте Указа Президента Республики Казахстан "О Концепции информационной безопасности Республики Казахстан до 2016 года"

Постановление Правительства Республики Казахстан от 30 сентября 2011 года № 1128

Правительство Республики Казахстан **ПОСТАНОВЛЯЕТ:**

внести на рассмотрение Президента Республики Казахстан проект Указа Президента Республики Казахстан "О Концепции информационной безопасности до 2016 года".

Премьер-Министр

Республики Казахстан *К. Масимов*

Указ Президент Республики Казахстан О Концепции информационной безопасности
Республики Казахстан до 2016 года

В целях обеспечения информационной безопасности Республики Казахстан

П О С Т А Н О В Л Я Ю :

1. Утвердить прилагаемую Концепцию информационной безопасности Республики Казахстан до 2016 года (далее - Концепция).

2. Центральным государственным и местным исполнительным органам, а также государственным органам, непосредственно подчиненным и подотчетным Президенту Республики Казахстан:

1) руководствоваться в своей деятельности Концепцией и обеспечить принятие своевременных мер по ее реализации;

2) принять иные меры, вытекающие из настоящего Указа.

3. Контроль за исполнением настоящего Указа возложить на Администрацию Президента Республики Казахстан.

4. Настоящий Указ вводится в действие со дня подписания.

Президент

Республики Казахстан *Н. Назарбаев*

У Т В Е Р Ж Д Е Н А
Указом Президента
Республики Казахстан
от " " 2011 года №

Концепция
информационной безопасности
Республики Казахстан до 2016 года Содержание

1. Видение развития обеспечения информационной безопасности Республики Казахстан

Концепция информационной безопасности Республики Казахстан (далее - Концепция) разработана в целях обеспечения интересов общества и государства в информационной сфере, а также защиты конституционных прав гражданина.

Концепция отвечает основным положениям Стратегии развития Республики Казахстан до 2030 года "Процветание, безопасность и улучшение благосостояния всех казахстанцев", в которой обеспечение информационной безопасности как составляющей национальной безопасности определено одним из основных долгосрочных приоритетов.

Концепция основана на оценке текущей ситуации и определяет государственную политику, перспективы деятельности государственных органов в области обеспечения информационной безопасности.

Концепция разработана в соответствии с Конституцией Республики Казахстан от 30 августа 1995 года и законами Республики Казахстан от 26 июня 1998 года "О национальной безопасности Республики Казахстан", от 15 марта 1999 года "О государственных секретах", от 13 июля 1999 года "О противодействии терроризму", от 7 января 2003 года "Об электронном документе и электронной цифровой подписи", от 11 января 2007 года "Об информатизации", от 9 ноября 2004 года "О техническом регулировании", от 11 января 2007 года "О лицензировании", от 23 июля 1999 года "О средствах массовой информации", от 5 июля 2004 года "О связи".

При разработке Концепции также учтен имеющийся международный опыт в

области обеспечения информационной безопасности, в частности Российской Федерации, Республики Таджикистан. Аналогичный документ - Доктрина информационной безопасности - в Российской Федерации, Концепция информационной безопасности - в Республике Таджикистан были утверждены в сентябре 2000 года и в ноябре 2003 года соответственно. Этот документ также устанавливает систему взглядов на цели, задачи, принципы и основные направления обеспечения информационной безопасности в Российской Федерации и в субъектах Российской Федерации. В Концепции информационной безопасности Республики Казахстан выдержан соответствующий международному опыту комплексный подход реализации вопросов обеспечения информационной безопасности, включающий законодательное, нормативно-методическое, организационное, технологическое и кадровое обеспечение.

Также в положения Концепции информационной безопасности РК включены основные направления Концепции сотрудничества государств-участников Содружества Независимых Государств в сфере обеспечения информационной безопасности, подписанной в г. Бишкек 10 октября 2008 года, Соглашения между правительствами государств-членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности, ратифицированного Законом Республики Казахстан от 1 июня 2010 года "О ратификации Соглашения между правительствами государств-членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности".

Концепция выражает совокупность официальных взглядов на сущность и содержание деятельности Республики Казахстан по обеспечению информационной безопасности государства и общества, их защите от внутренних и внешних угроз. Концепция определяет задачи, приоритеты, направления и ожидаемые результаты в области обеспечения информационной безопасности личности, общества и государства . Она является основой для конструктивного взаимодействия органов государственной власти, бизнеса и общественных объединений для защиты национальных интересов Республики Казахстан в информационной сфере. Концепция призвана обеспечить единство подходов к формированию и реализации государственной политики обеспечения информационной безопасности, а также методологическую основу для совершенствования нормативно-правовых актов, регулирующих данную сферу.

Растущая степень открытости экономик, свободы перемещения товаров, капиталов и трудовых ресурсов, межличностного взаимодействия размывает грань между внутренними и внешними политическими, экономическими и информационными процессами.

Технологическая эволюция становится источником принципиально новых угроз, предоставляя недоступные ранее возможности негативного влияния на личность,

общество и государство.

Усиливается роль и влияние средств массовой информации и глобальных коммуникационных механизмов. Информационные технологии нашли широкое применение в управлении важнейшими объектами жизнеобеспечения, которые становятся более уязвимыми перед случайными и преднамеренными воздействиями.

Настоящая Концепция определяет основные стратегические цели, задачи и направления, стоящие перед страной в целях обеспечения ее информационной безопасности.

Используемые термины и определения

Информационная безопасность страны в данном документе рассматривается с двух взаимосвязанных аспектов: технического и социального.

Технический аспект подразумевает обеспечение защиты национальных информационных ресурсов, информационных систем, информационно-телекоммуникационной инфраструктуры от неавторизованного доступа, использования, раскрытия, нарушения, изменения, прочтения, проверки, записи или уничтожения для обеспечения целостности, конфиденциальности и доступности информации.

Социальный аспект заключается в защите национального информационного пространства и систем распространения массовой информации от целенаправленного негативного информационного и организационного воздействия, могущего причинить ущерб национальным интересам Республики Казахстан.

Информационная война - противоборство между государствами в информационном пространстве с целью нанесения ущерба информационным системам, процессам и ресурсам, критически важным и другим структурам, подрыва политической, экономической и социальной систем, массированной психологической обработки населения для дестабилизации общества и государства, а также принуждения государства к принятию решений в интересах противоборствующей стороны.

Информационная инфраструктура - совокупность информационных ресурсов и систем, технических средств информационно-коммуникационных сетей используемых для формирования, создания, преобразования, передачи, использования и хранения информации.

Информационное пространство - сфера деятельности, связанная с формированием, созданием, преобразованием, передачей, использованием, хранением информации, оказывающая воздействие, в том числе на индивидуальное и общественное сознание, информационную инфраструктуру и собственно информацию.

Информационная преступность (киберпреступность) - вид уголовной преступности, подразумевающий уголовно-наказуемые деяния с использованием информационных

технологий.

Информационный терроризм - использование информационных ресурсов и (или) воздействие на них в информационном пространстве в террористических целях.

Критически важные объекты информатизации - объекты информационной и телекоммуникационной инфраструктуры, прекращение или нарушение функционирования которых приводит к чрезвычайной ситуации или к значительным негативным последствиям для обороны, безопасности, международных отношений, экономики, другой сферы хозяйства или инфраструктуры страны, либо для жизнедеятельности населения, проживающего на соответствующей территории, на длительный период времени.

Контент - любое информационно-значимое наполнение средств массовой коммуникации. Под средствами массовой коммуникации понимается совокупность средств массовой информации (пресса, радио, телевидение, интернет) и средств массового воздействия (театр, кино, цирк, зрелища, литература).

Общественное сознание - духовная жизнь общества в совокупности чувств, настроений, взглядов, идей, теорий, отражающих общественное бытие и влияющих на него. Общественное сознание рассматривается как самостоятельная целостная система, не сводимая к сумме составляющих его индивидов.

Электронные информационные ресурсы - информация, хранимая в электронном виде (информационные базы данных), содержащаяся в информационных системах.

Анализ текущей ситуации

Процесс поступательного развития Республики Казахстан, как суверенного и процветающего государства, невозможно рассматривать вне контекста имеющихся общемировых тенденций и реалий. Человечество вступило в стадию кардинальных социальных, экономических, политических и иных изменений, характеризующихся быстрым развитием информационной сферы, становящейся одним из ключевых факторов, влияющих на жизнь людей, обществ и государств.

Ведущие государства мира находятся в процессе построения информационного общества, основывающегося на новых технологиях, новых методах и новых подходах. В конечном итоге их использование должно способствовать адекватной новым реалиям реализации конституционных прав граждан, улучшению благосостояния населения, повышению конкурентоспособности компаний. Для государственных органов информационное общество позволит эффективно преобразовать процедуры предоставления услуг гражданам.

Таким образом, степень развитости информационного общества непосредственно влияет на процесс функционирования государственных институтов, экономику и обороноспособность каждой страны. В реалиях современного мира наличие

адекватного потребностям граждан информационного общества является необходимым условием состоятельности государства.

Основными национальными интересами Республики Казахстан в информационной сфере являются:

1) реализация конституционных прав граждан на получение и распространение информации;

2) формирование и поступательное развитие информационного общества;

3) равноправное участие государства в мировом информационном обмене;

4) опережающее развитие информационно-коммуникационных технологий;

5) эффективное и своевременное информационное обеспечение органов государственной власти;

6) недопущение фактов утрат и разглашения сведений, составляющих государственные секреты, а также иной охраняемой информации;

7) обеспечение надежности и устойчивости функционирования критически важных информационных систем, ресурсов и поддерживающей инфраструктуры.

В результате бурного развития процессов информатизации общества и государства, в т.ч. опережающего развития "электронного правительства", в Республике Казахстан сложились предпосылки для построения информационного общества. Так, согласно данным рейтинга готовности стран к использованию технологий электронного правительства Организации Объединенных Наций за 2010 год Казахстан занял 46 место из 192 стран (81 место в 2008 году).

Вместе с тем развитие вышеуказанных процессов привело к усилению существовавших и появлению новых проблем и угроз информационной безопасности страны.

В межгосударственных отношениях нарастает тенденция использования информационного давления как действенного механизма глобальной конкуренции. Использование различных средств информационной войны и информационной экспансии стали неотъемлемым инструментом решения политических конфликтов. Активно используется методы блокирования Интернет-СМИ путем проведения распределенных компьютерных атак "отказ в обслуживании". Ведущие страны мира уже создали в составе своих вооруженных сил информационные войска и не скрывают намерений их активного использования.

Развитые страны мира, имеющие возможность осуществления глобального мониторинга распространяемой информации используют его результаты для получения односторонних преимуществ в политических, экономических, военных, экологических и прочих аспектах межгосударственных отношений.

Экстремистскими и террористическими организациями и группами все активнее используются возможности глобальных информационно-коммуникационных сетей для пропаганды своей идеологии, вербовки и обучения единомышленников, поддержания

связи и финансирования различных террористических групп. Распространение радикальных идей различного толка среди молодежи Казахстана принимает угрожающий характер. Все чаще отмечаются случаи, когда граждане Казахстана под влиянием целенаправленной пропаганды, в т.ч. посредством сети Интернет участвуют в деятельности незаконных вооруженных формирований в различных горячих точках. Растет угроза использования компьютерных атак на информационные системы государства как метода осуществления террористической деятельности. Подобные атаки уже неоднократно были зафиксированы в других, в том числе дружественных Республике Казахстан, странах.

Существенную проблему составляет распространение информационной преступности (киберпреступности), в том числе деятельность организованных транснациональных преступных групп. Специфика киберпреступлений заключается в их весьма высокой латентности. Вследствие этого, официально зарегистрированные преступления с использованием современных информационно-коммуникационных технологий составляют лишь незначительную часть от реально совершенных. Борьба с информационной преступностью требует от правоохранительных органов адекватного оперативного реагирования путем проведения совместных скоординированных действий со специальными службами и правоохранительными органами зарубежных стран.

Несмотря на то, что этот вид преступности не стал столь распространенным на территории Казахстана, на сегодняшний день его динамика характеризуется устойчивой тенденцией роста использования телекоммуникационных технологий, изощренностью, появлением новых способов совершения преступлений, доказательство которых сильно затруднено отсутствием необходимых правовых, организационных и технических инструментов.

Назрела необходимость выработки новых концептуальных мер противодействия преступлениям и правонарушениям в сфере информационных технологий, основанных на совершенствовании нормативной правовой базы, осуществлении технического перевооружения, широкого привлечения общественности, поиска новых форм и методов противодействия.

Усиливается роль и влияние глобальных средств массовой информации и коммуникационных механизмов на развитие экономической, политической и социальной ситуации в различных странах мира. Фундаментальные перемены, произошедшие в последние годы в странах с различными экономическими и политическими условиями, указывают на ключевую роль в данных процессах новых технологий управления массами, в том числе посредством использования информационно-коммуникационных технологий: социальных сетей, массовой рассылки коротких сообщений (SMS) посредством мобильных телефонов и специальных сайтов. Широкое использование населением Казахстана социальных

сетей и блогов создает возможность их использования для оказания целенаправленного воздействия на внутриполитическую ситуацию в ущерб национальным интересам Республики Казахстан, в т.ч. для организации массовых беспорядков, волнений и иных чрезвычайных ситуаций политического и социального характера.

В связи с открытостью национального информационного пространства и популярностью зарубежных средств массовой информации, в т.ч. телевидения и интернет-ресурсов (почтовых служб, социальных сетей, блогов и видеопорталов), возникает реальная угроза информационного влияния на общественное сознание населения. Информационное влияние может выражаться как в виде прямого навязывания идей, противоречащих национальным интересам Республики Казахстан, так и в виде создания определенного информационного фона, искусственно поддерживаемого путем манипулирования информацией или ее тенденциозным комментированием. Для противодействия подобным манипулированием общественным сознанием требуется серьезно улучшить эффективность государственной информационной политики, увеличить открытость государственных органов, повысить обеспеченность права граждан на информацию.

Серьезные угрозы несет в себе проблема неконкурентоспособности отечественного контента. Его качество остается недостаточным для полноценной конкуренции с иностранным информационным и развлекательным продуктом. В условиях открытости национального информационного пространства это приводит к его низкой популярности. В свою очередь, низкая популярность не позволяет привлечь значимые инвестиции в его производство, что приводит к крайней недостаточности производства отечественного контента.

Отсутствие соответствующих потребностям государства, бизнеса и общества отечественных информационных технологий приводит к вынужденному использованию иностранного оборудования и информационных систем. В результате этого повышается вероятность несанкционированного доступа к базам и банкам данных, а также возрастает зависимость страны от иностранных производителей компьютерной и телекоммуникационной техники и программного обеспечения.

Проверки состояния защищенности государственных баз данных, включенных в состав "электронного правительства", указывают на отсутствие адекватного правового, организационного и технического режима защиты персональных данных граждан. Отсутствие соответствующих механизмов создает предпосылки для злоупотребления персональными данными в криминальных целях, в т.ч. подделке документов, мошенничеству, незаконному копированию и распространению различных баз данных.

Недостаточно эффективно функционирует система защиты информации. В частности, слабо используются технические средства защиты информации от несанкционированного доступа и копирования. Не реализуются политики безопасности и организационно-технические меры, противодействующие утечке информации, что

приводит к злоупотреблениям полномочиями в корыстных целях. Потерям важной информации способствуют бессистемность защиты данных и слабая координация мер по защите информации в общегосударственном масштабе, ведомственная разобщенность в обеспечении целостности и конфиденциальности информации.

Все более остро встает проблема нехватки квалифицированных кадров в информационно-коммуникационной отрасли, в том числе и в сфере информационной безопасности. Согласно данным компании IDC, одной из лидирующих аналитических компаний на рынке информационно-коммуникационных технологий, количество ИТ-специалистов на 100 тыс. жителей в Казахстане в 2010 году составило 113 человек, что более чем в 12 раз ниже, чем в Малайзии и в 29 раз ниже, чем в США.

Требуется дальнейшее совершенствование процессов и подходов обучения, повышения квалификации специалистов государственных органов, организаций, занятых в сфере защиты государственных секретов, обеспечения информационной безопасности.

Определенную угрозу составляет сравнительно низкий уровень общей правовой и информационной культуры, в т.ч. навыков безопасного использования киберпространства в казахстанском обществе.

Существенно отстает от потребностей текущего дня правовое обеспечение информационной сферы. Недостаточно проработаны правовые механизмы, регулирующие информационные правоотношения, возникающие при осуществлении поиска, получения и потребления информации, информационных ресурсов, информационных продуктов, информационных услуг. Нуждаются в улучшении и актуализации правовые механизмы, регулирующие процессы производства, передачи и распространения информации, информационных ресурсов, информационных продуктов, информационных услуг. Особо остро стоит вопрос с регулированием информационных правоотношений, возникающих при создании и применении информационных систем, их сетей, средств обеспечения, телекоммуникационной инфраструктуры. Современное состояние правового обеспечения противодействия информационным преступлениям также характеризуется недостаточной согласованностью используемых правовых механизмов, фрагментарностью деятельности субъектов законодательной инициативы по их развитию и совершенствованию, недостаточной эффективностью, противоречивостью правовых норм, несовершенством правовой статистики.

Вышеуказанные проблемы в правовом обеспечении информационной сферы создают серьезную угрозу информационной безопасности государства. На повестку дня остро встает вопрос о необходимости формирования в Республике Казахстан отдельной правовой отрасли - информационного права.

В последнее время актуализируется проблема равноправного участия Республики Казахстан в международном информационном обмене и в процессах международного

регулирования информационной безопасности. Необходимость отстаивания национальных интересов требует повышения активности государственных органов в рамках деятельности существующих международных организаций.

Таким образом, текущее состояние информационной безопасности характеризуется следующими угрозами:

1) нарушения функционирования критически важных объектов информатизации, в том числе различных государственных и негосударственных информационных систем и поддерживающей их инфраструктуры;

2) несоответствия уровня производства, внедрения и использования современных информационно-коммуникационных технологий объективным потребностям общества;

3) возможности деструктивного информационного воздействия на общественное сознание и государственные институты, наносящего ущерб национальным интересам страны;

4) недостаточности развития и низкой конкурентоспособности отечественных информационных ресурсов и отечественного контента.

Внутренними источниками угроз информационной безопасности являются:

1) зависимость Республики Казахстан от импорта информационных технологий, средств информатизации и защиты информации, неконтролируемое использование которых может причинить ущерб национальным интересам страны;

2) несоответствие качества отечественного контента мировому уровню;

3) допущение работниками государственных органов и организаций фактов грубых нарушений режима секретности, таких, как утрата секретных документов и разглашение сведений, составляющих государственные секреты Республики Казахстан, вследствие "человеческого фактора";

4) распространение недостоверной или умышленно искаженной информации, способной причинить ущерб национальным интересам Республики Казахстан;

5) недостаточное развитие системы правового регулирования информационной сферы;

6) рост преступности с использованием информационно-коммуникационных технологий;

7) недостаточная эффективность информационного обеспечения государственной политики;

8) несовершенство системы обеспечения безопасности критически важных объектов информатизации.

Внешними источниками угроз информационной безопасности являются:

1) открытость и уязвимость национального информационного пространства от внешнего воздействия;

2) нарастание информационного противоборства между ведущими мировыми центрами силы, подготовка и ведение зарубежными государствами борьбы в

информационном пространстве;

3) развитие технологий манипулирования информацией;

4) рост транснациональной преступности и экстремисткой, террористической деятельности с использованием информационно-коммуникационных технологий;

5) попытки несанкционированного доступа извне к информационным ресурсам Республики Казахстан, приводящие к причинению ущерба ее национальным интересам

.

Цели и задачи

Целью Концепции является создание национальной системы информационной безопасности, обеспечивающей защиту национальных интересов Республики Казахстан в информационной сфере.

Для достижения указанной цели необходимо решить следующий комплекс задач:

1) развитие системы управления информационной безопасностью, позволяющей обеспечить защищенность национальной информационной инфраструктуры страны и национального информационного пространства;

2) разработка и реализация единой государственной технической политики в сфере обеспечения информационной безопасности, в т.ч. развитие и укрепление национальной системы защиты информации;

3) защита прав личности и интересов общества и государства в информационной сфере;

4) развитие отечественного информационного пространства;

5) совершенствование законодательства, регулирующего информационную сферу;

6) обеспечение активного участия Республики Казахстан в процессах создания и использования глобальных информационных сетей и систем (международное сотрудничество).

Организационное обеспечение вопросов реализации настоящей Концепции возлагается на уполномоченные государственные органы.

Государственные органы, организации принимают меры по включению соответствующих мероприятий, вытекающих из настоящей Концепции, в стратегические планы, программные документы. Обеспечение взаимодействия государственных органов, международных и других организаций в области информационной безопасности будет производиться посредством Межведомственной комиссии по координации работ в сфере информатизации.

Финансовое и материально-техническое обеспечение реализации Концепции будет осуществляться за счет и в пределах средств, предусматриваемых в республиканском и местном бюджетах.

Периоды исполнения и ожидаемые результаты

Эффективность реализации Концепции зависит от уровня консолидации усилий заинтересованных государственных органов, коммерческих и общественных организаций, широкой общественности.

В целом, обеспечение информационной безопасности Республики Казахстан будет осуществлено в течение 5 лет.

По результатам реализации Концепции будет достигнуто следующее:

1) развитие информационных технологий и телекоммуникаций;

2) будет обеспечено недопущение инцидентов, влекущих за собой несанкционированный доступ, потерю или искажение информации;

3) будет обеспечена ежегодная 100 % аттестация государственных информационных систем по требованиям информационной безопасности;

4) доля граждан, получающих основную информацию из отечественных СМИ, в 2012 году составит - 35 %, в 2013 - 40 %, в 2014 году - 45 %, в 2015 году - 50 %, в 2016 году - 55 %;

5) доля отечественного контента в СМИ будет поддержана на уровне 50 %;

6) увеличится доля граждан, имеющих доступ к сети Интернет, которая составит в 2012 году - 34,6 %, в 2013 - 35,2 %, в 2014 году - 35,8 %, в 2015 году - 36 %, в 2016 году - 36,6 %;

7) к 2016 году уровень обеспечения устранения простоя информационных систем из-за проблем информационной безопасности сократится до 20 минут;

8) будет обеспечено производство отечественного компьютерного оборудования, комплектующих, периферийных устройств и программных продуктов;

9) повысится уровень инновационной активности промышленных предприятий;

10) будет усовершенствована нормативно-правовая база, регулирующая информационную сферу, в том числе в рамках международного сотрудничества;

11) будет совершенствована система кадрового обеспечения в области информационной безопасности и защиты государственных секретов.

Реализация настоящей Концепции будет способствовать:

1) реализации конституционных прав граждан на получение, хранение и распространение полной, достоверной и своевременной информации;

2) равноправному участию Республики Казахстан в мировых информационных отношениях;

3) эффективному информационному обеспечению государственной политики;

4) обеспечению надежности и устойчивости функционирования критически важных информационных систем.

2. Основные принципы и общие направления развития обеспечения информационной безопасности Республики Казахстан

Реализация задач Концепции требует развития трех направлений:
1) законодательного и нормативно-методического;
2) организационно-распорядительного и организационно-технического;
3) кадрового.

По направлению законодательного и нормативно-методического обеспечения требуется решение вопросов развития партнерства государства и общества по координации усилий в области обеспечения национальных интересов в информационной сфере, в том числе определению модели взаимодействия государственного и негосударственного секторов для противодействия угрозам информационной безопасности на национальном уровне, в том числе противодействия информационному терроризму и информационной преступности, разработка единой государственной технической политики в сфере обеспечения информационной безопасности, принятию законодательных, институциональных мер по развитию СМИ. В частности, будут определены ответственные органы по выработке политики информационной безопасности страны, разграничены сферы ответственности государственных органов, задействованных в области обеспечения информационной безопасности и защиты государственных секретов, а также созданы механизмы их эффективной межведомственной координации. Кроме того, будет определен перечень критически важных объектов информатизации, в том числе информационных систем и ресурсов, влияющих на информационную безопасность Республики Казахстан.

При этом, Единая государственная техническая политика в сфере обеспечения информационной безопасности (далее - ГТПИБ) призвана обеспечить выработку и реализацию единых стандартов в области обеспечения требований информационной безопасности к государственным и негосударственным информационным системам, ресурсам и их поддерживающей инфраструктуре. В частности, требуется актуализация действующих нормативных правовых и технических актов в области информационно-технического развития и защиты информации, в том числе защиты государственных секретов. Будет проведена градация информационных систем и ресурсов по уровням информационной безопасности, усовершенствованы процедуры сертификации технических и программных средств, аттестации информационных систем на соответствие требованиям информационной безопасности, развито международное сотрудничество в данной области, выработаны государственные меры по повышению ответственности за состояние информационной безопасности и защиты государственных секретов.

Кроме того, реалии сегодняшнего дня требуют выделения существующих норм законодательства в отдельную правовую отрасль - информационное право, разработки

законодательства по вопросам защиты критической информационной инфраструктуры, внесения изменений в существующее законодательство по вопросам отнесения отдельных видов информационных правонарушений к уголовно-наказуемым деяниям, также требуется дополнительная правовая регламентация вопросов соблюдения авторского права в информационно-коммуникационных сетях, совершенствование законодательства, регулирующего вопросы защиты персональных данных, совершенствование международных правовых норм в области информационной безопасности и защиты государственных секретов для обеспечения соблюдения национальных интересов Республики Казахстан.

Принимая во внимание трансграничный характер вопросов обеспечения информационной безопасности требуется дальнейшее совершенствование международного сотрудничества в данной области, соответствующего принципам равноправного международного информационного обмена.

Требуется разработка международных правовых норм, регулирующих межгосударственные отношения в области использования глобальной информационной инфраструктуры, совершенствования взаимодействия правоохранительных органов Республики Казахстан и иностранных государств в области предупреждения, выявления, пресечения и ликвидации последствий использования информационных и телекоммуникационных технологий в террористических и иных преступных целях, гармонизация национальной системы стандартов и сертификации в этой сфере с международной системой.

По направлению организационно-распорядительного и организационно-технического обеспечения требуется реализация комплекса мероприятий по обеспечению информационной безопасности критически важных объектов информатизации, обеспечению единой государственной технической политики в сфере информационной безопасности, в том числе национальной системы защиты информации. Для решения данного вопроса требуется создание единой государственной системы мониторинга информационного пространства, создание информационной системы и инфраструктуры Оперативного центра обеспечения информационной безопасности. Кроме того, немаловажным является вопрос инновационного развития в области обеспечения информационной безопасности, в частности, создание благоприятных условий для развития инновационной деятельности, основ отечественной базы НИОКиТР (научно-исследовательские опытно-конструкторские и технологические работы) и производства программных и технических средств обработки и защиты информации. Также требуется создание единой инфокоммуникационной сети государственных органов, создание оперативного центра обеспечения информационной безопасности (ОЦ) для координации усилий по защите критической инфраструктуры в сфере информационных технологий, развитие Единого шлюза доступа государственных органов к сети Интернет, Единой

электронной почтовой системы для государственных органов, создание не менее двух территориально разнесенных центров хранения резервных баз данных государственных органов, развитие национальной системы идентификации в киберпространстве Республики Казахстан, создание узлов кибербезопасности, повышение качества и надежности систем обеспечения информационной безопасности "электронного правительства", направленных на недопущение несанкционированного доступа, потери, искажения информации.

Кроме того, государственными органами будет обеспечено проведение аттестации государственных информационных систем по требованиям информационной безопасности, что также будет способствовать уменьшению времени простоя информационных систем.

Также требуется проведение целенаправленной политики по выявлению и недопущению скрытого воздействия на общественное сознание со стороны других государств, транснациональных корпораций, различных неформальных структур, в том числе через социальные сети, активизация противодействия распространению идеологии терроризма, религиозного и этнического экстремизма, сепаратизма и других антиобщественных проявлений через системы распространения массовой информации.

Будет внедрена оптимальная модель развития и регулирования казахстанского сегмента глобальной информационной сети Интернет, выработаны механизмы стимулирования производства позитивного содержательного контента, развитию отечественных интернет-СМИ, модернизации телекоммуникационной инфраструктуры.

Реализация данных мероприятий направлена на усиление присутствия казахстанских СМИ в центрально-азиатском и международном информационном пространстве в целях продвижения позитивного имиджа страны.

Кроме того, будет развито международное сотрудничество в области проведения исследовательских проектов по приоритетным направлениям развития науки, технологий и техники.

По направлению кадрового обеспечения требуется решение вопросов совершенствования системы подготовки кадров в области обеспечения информационной безопасности и защиты государственных секретов, кадрового обеспечения подразделений правоохранительных органов, в том числе занятых вопросами противодействия информационному терроризму и информационной преступности. Немаловажным остается вопрос повышения эффективности учебных и образовательных программ по вопросам информационной безопасности и защиты государственных секретов.

3. Перечень нормативных правовых актов, посредством которых предполагается реализация Концепции

Основными нормативными правовыми актами, посредством которых планируется реализация Концепции являются:

1) отраслевая Программа по развитию системы защиты государственных секретов Республики Казахстан на 2011-2014 годы, утвержденная постановлением Правительства Республики Казахстан;

2) отраслевая Программа по обеспечению информационной безопасности Республики Казахстан на 2011-2014 годы, утвержденная постановлением Правительства Республики Казахстан от 31 января 2011 года № 45 дсп;

3) стратегические планы государственных органов;

4) законы.