О Концепции информационной безопасности Республики Казахстан

Утративший силу

Указ Президента Республики Казахстан от 10 октября 2006 года № 199. Утратил силу Указом Президента Республики Казахстан от 11 апреля 2011 года № 5

Сноска. Утратил силу Указом Президента РК от 11.04.2011 № 5.

В целях обеспечения информационной безопасности Республики Казахстан

ПОСТАНОВЛЯЮ:

1. Одобрить прилагаемую Концепцию информационной безопасности Республики Казахстан.

2. Государственным органам и организациям Республики Казахстан руководствоваться в своей деятельности положениями настоящей Концепции.

3. Настоящий Указ вводится в действие со дня подписания.

П р е з и д е н т

Республики Казахстан

О Д О Б Р Е Н А

У к а з о м П р е з и д е н т а
Р е с п у б л и к и К а з а х с т а н
от 10 октября 2006 года N 199

КОНЦЕПЦИЯ
информационной безопасности Республики Казахстан

Введение

В Послании Президента страны народу Казахстана от 10 октября 1997 года " Казахстан - 2030. Процветание, безопасность и улучшение благосостояния всех казахстанцев" в качестве долгосрочного приоритета определена национальная безопасность, одной из составляющих которой является информационная б е з о п а с н о с т ь .

Динамика развития информационных технологий в социально-экономической и культурной жизни общества и государства предъявляет повышенные требования к решению вопросов информационной б е з о п а с н о с т и .

Обеспечение информационной безопасности государства требует использования комплексного подхода, включающего организационные,

технические, программные, социальные механизмы, способные реализовать конституционные права и свободы человека и гражданина в области получения информации, пользования ею в целях защиты конституционного строя, суверенитета и территориальной целостности Республики Казахстан, политической, экономической и социальной стабильности, законности и правопорядка, развития взаимовыгодного международного сотрудничества в области информационной безопасности.

1. Общие положения

Концепция информационной безопасности Республики Казахстан (далее - Концепция) разработана на основании Конституции Республики Казахстан и законов 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 борьбе с терроризмом ", от 7 января 2003 года "Об электронном документе и электронной цифровой подписи", от 8 мая 2003 года " Об информатизации " и от 18 февраля 2005 года " О противодействии экстремизму ", Концепции развития конкурентоспособности информационного пространства Республики Казахстан на 2006-2009 годы, одобренной Указом Президента Республики Казахстан от 18 августа 2006 года N 163.

Также при разработке Концепции учтены международный опыт в области информационной безопасности и положения Концепции информационной безопасности государств-участников Содружества Независимых Государств в военной сфере от 4 июня 1999 года.

Концепция служит основой при формировании и реализации единой государственной политики Республики Казахстан в области обеспечения информационной безопасности, ее положения будут учитываться при создании и развитии единого информационного пространства Казахстана и дальнейшем совершенствовании государственной политики в области информатизации.

Государственная политика в области обеспечения информационной безопасности Республики Казахстан (далее - государственная политика) является открытой и предусматривает информированность общества о деятельности государственных органов и общественных институтов в области информационной безопасности с учетом ограничений, предусмотренных действующими законодательными актами Республики Казахстан. Она основывается на обеспечении прав физических и юридических лиц на свободное создание, поиск, получение и распространение информации любым законным способом.

Государство исходит из того, что информационные ресурсы являются

объектом собственности, и способствует введению их в хозяйственный оборот при соблюдении законных интересов собственников, владельцев и распорядителей информационных ресурсов.

Государство считает приоритетным развитие современных информационных и телекоммуникационных технологий и технических средств, способных обеспечить создание национальных телекоммуникационных сетей и международный информационный обмен.

Государственная политика не допускает монополизма государственных органов и организаций в области обеспечения информационной безопасности, за исключением сферы защиты государственных секретов.

2. Состояние информационной безопасности Республики Казахстан

Происходящие в настоящее время процессы преобразования в политической жизни и экономике Казахстана оказывают непосредственное влияние на состояние его информационной безопасности. При этом возникают новые факторы, которые необходимо учитывать при оценке реального состояния информационной безопасности и определении ключевых проблем и направлений в этой области.

Указанные факторы можно разделить на политические, экономические и организационно-технические.

Политическими факторами являются:

изменение геополитической обстановки в различных регионах мира;

информационная экспансия развитых стран мира, осуществляющих глобальный мониторинг мировых политических, экономических, военных, экологических и других процессов, распространяющих информацию в целях получения односторонних преимуществ;

становление новой казахстанской государственности на основе принципов демократии, законности, информационной открытости, совершенствования системы обеспечения безопасности страны;

возникновение внутриполитических кризисов: конфликты между ветвями власти, субъектами территориального государственного устройства, покушения на охраняемых лиц;

деятельность внутриполитических блоков, союзов, альянсов, создание новых военно-политических объединений, влияющих на геополитическую расстановку сил в мире;

стремление Казахстана к более тесному сотрудничеству с зарубежными странами в процессе проведения реформ;

терроризм и экстремизм, обострение криминогенной обстановки, рост числа

компьютерных преступлений, особенно в кредитно-финансовой сфере.

Среди экономических факторов наиболее существенными являются:

активное вхождение Казахстана в мировое экономическое пространство, появление множества отечественных и зарубежных негосударственных структур - производителей и потребителей информации, средств информатизации и защиты информации, включение информационной продукции в систему товарных отношений;

расширяющаяся кооперация с зарубежными странами в интересах развития информационной инфраструктуры Казахстана;

коммуникационная глобализация, оказывающая растущее воздействие на развитие экономических процессов во всем мире;

отставание Казахстана в развитии и внедрении новейших информационных технологий, которые во все большей степени определяют уровень экономико-технологического развития в современном мире.

Из организационно-технических факторов определяющими являются:

недостаточная нормативная правовая база в сфере информационных отношений, в том числе в области обеспечения информационной безопасности;

слабое регулирование государством процессов функционирования и развития рынка средств информатизации, информационных продуктов и услуг в Казахстане;

широкое использование в сфере государственного управления, кредитно-финансовой и других сферах не защищенных от утечки информации и внешнего воздействия импортных технических и программных средств для хранения, обработки, передачи и защиты информации;

рост объемов информации, передаваемой по открытым каналам связи и системам передачи данных.

Анализ современного состояния информационной безопасности в Казахстане показывает, что ее уровень в настоящее время не соответствует потребностям человека, общества и государства.

Сегодняшние условия политического и социально-экономического развития страны вызывают обострение противоречий между потребностями общества в расширении свободного обмена информацией и необходимостью сохранения отдельных ограничений на ее распространение.

Для обеспечения государственных органов полной, достоверной и своевременной информацией требуются принятие обоснованных решений, в том числе для защиты государственных информационных ресурсов, а также разработка отечественных средств защиты информации и системы подтверждения соответствия импортируемых технических средств установленным требованиям.

Негативное влияние на организацию информационной безопасности в республике оказывает недостаточное количество профессиональных специалистов и области защиты информации.

Требуется дальнейшая проработка вопросов противодействия техническим разведкам, защиты от информационного оружия и совершенствования нормативной правовой базы в данной сфере.

В этих целях необходима комплексная координация мер по защите информации в общегосударственном масштабе и на ведомственном уровне для обеспечения целостности и конфиденциальности информации.

С возрастанием роли Интернета в информационном пространстве возникает необходимость защиты прав и свобод человека и общества от информации, пропагандирующей насилие и жестокость, навязывания им ложной и недостоверной информации, от целенаправленного формирования негативного мировоззрения молодого поколения. При этом источники внешних угроз могут находиться вне юрисдикции законодательства Республики Казахстан, что существенно затрудняет применение системы правовых мер.

Актуальной проблемой является отсутствие отечественных информационных технологий, что вынуждает массового потребителя приобретать импортную технику, не имеющую подтверждения соответствия требованиям информационной безопасности. Это представляет угрозу информационной безопасности баз и банков данных, а также возможной зависимости страны от иностранных производителей компьютерной и телекоммуникационной техники и информационной продукции.

Субъектами правоотношений в информационной сфере являются физические и юридические лица независимо от форм собственности.

Собственниками информации могут являться: государство (в лице государственных органов и организаций, должностных лиц), физические и юридические лица.

С точки зрения создания и использования информации субъекты информационных отношений могут выступать в качестве авторов, собственников, владельцев или пользователей.

Информация и информационные ресурсы могут являться вещной или интеллектуальной собственностью. Поэтому при обработке информации в информационных системах требуется обеспечивать не только конфиденциальность информации, но также ее целостность и доступность. Для электронных документов необходимо подтверждать электронной цифровой подписью подлинность каждого документа.

В отношении информации, содержащей сведения, составляющие государственные секреты, действует установленный режим секретности для всех

субъектов отношений. Собственником данной информации является государство .

Для обеспечения защиты информации с ограниченным доступом, собственником которой является государство, функционирует государственная система защиты информации.

Успешное функционирование современного общества всецело зависит от того, насколько эффективно организованы и отлажены информационные процессы, протекающие в нем. В этой связи все большее значение для Республики Казахстан приобретает объединение данных процессов в информационное пространство в рамках государства.

Единое информационное пространство позволит обеспечить удовлетворение информационных потребностей физических и юридических лиц, будет способствовать стимулированию деятельности производителей и потребителей информации, вхождению страны в мировое информационное пространство.

При формировании единого информационного пространства Республики Казахстан возрастает роль "электронного правительства", создание которого было предусмотрено Государственной программой формирования "электронного правительства" в Республике Казахстан на 2005-2007 годы, утвержденной Указом Президента Республики Казахстан от 10 ноября 2004 года N 1471. " Электронное правительство" позволит существенно повысить эффективность функционирования всех ветвей власти за счет обеспечения информационной поддержки их деятельности и динамичной организации информационного взаимодействия между ними, а также с субъектами экономики и населением.

В рамках Государственной программы формирования "электронного правительства" в Республике Казахстан на 2005-2007 годы создаются государственные базы данных "Физические лица", "Юридические лица", " Регистр недвижимости", "Адресный регистр", безопасность которых будет обеспечена в результате защищенного информационного взаимодействия между субъектами информационных отношений.

3. Цели и задачи обеспечения информационной безопасности

Основными целями обеспечения информационной безопасности являются:

создание и укрепление национальной системы защиты информации, в том числе в государственных информационных ресурсах;

защита государственных информационных ресурсов, а также прав человека и интересов общества в информационной сфере;

недопущение информационной зависимости Казахстана, информационной экспансии или блокады со стороны других государств, информационной

изоляции Президента, Парламента, Правительства и других государственных органов и организаций.

Основными задачами по обеспечению информационной безопасности Республики Казахстан являются:

совершенствование национального законодательства в области информационной безопасности;

выявление, оценка, прогнозирование источников угроз информационной безопасности, определение параметров разведдоступности защищаемых объектов;

разработка государственной политики обеспечения информационной безопасности, комплекса мероприятий и методов ее реализации;

координация деятельности государственных органов и организаций в области обеспечения информационной безопасности;

развитие системы обеспечения информационной безопасности, совершенствование ее организации, форм, методов и средств нейтрализации угроз информационной безопасности, ликвидации последствий ее нарушений;

обеспечение активного участия Казахстана в процессах создания и использования глобальных информационных сетей и систем;

создание системы противодействия техническим разведкам путем разработки и совершенствования нормативной правовой и методологической базы по противодействию техническим разведкам.

4. Объекты, угрозы, методы, средства и основные направления обеспечения информационной безопасности

К объектам информационной безопасности Республики Казахстан относятся:

права физических и юридических лиц, государства на получение, распространение и использование информации, защиту конфиденциальной информации и интеллектуальной собственности;

информационные ресурсы вне зависимости от форм хранения, содержащие сведения, составляющие государственные секреты, коммерческую тайну и другую конфиденциальную информацию, а также открытую (общедоступную) информацию;

система формирования, хранения, распространения и использования информационных ресурсов, включающая в себя информационные системы различного класса и назначения, библиотеки, архивы, базы и банки данных, информационные технологии, регламенты и процедуры сбора, обработки, хранения и передачи информации, научно-технический и обслуживающий персонал;

система формирования общественного сознания (мировоззрение, политические взгляды, моральные ценности и прочие), базирующаяся на средствах массовой информации и пропаганды;

сети телекоммуникаций специального назначения, а также спутниковые системы связи;

открытия, незапатентованные технологии, математические и технологические алгоритмы, промышленные образцы, полезные модели и экспериментальное оборудование;

системы управления сложными исследовательскими комплексами (ядерные реакторы, ускорители элементарных частиц, космические комплексы и так далее);

средства и системы информатизации (средства вычислительной техники, информационно-вычислительные комплексы, сети и системы), программные средства (операционные системы, системы управления базами данных, другое общесистемное и прикладное программное обеспечение), автоматизированные системы управления, системы связи и передачи данных государственных органов и организаций, осуществляющие прием, обработку, хранение и передачу информации, содержащей государственные секреты;

системы принятия политических решений.

Угрозы информационной безопасности Республики Казахстан в зависимости от их происхождения можно разделить на внешние и внутренние.

Источниками угроз информационной безопасности являются:

отдельные иностранные политические, экономические, военные и информационные структуры;

разведывательные и специальные службы иностранных государств;

международные террористические и экстремистские организации;

незаконные политические, религиозные и экономические структуры деструктивной направленности;

организованные криминальные сообщества и группы;

отдельные физические и юридические лица;

стихийные бедствия и катастрофы.

К внешним угрозам относятся:

неконструктивная политика иностранных государств в области глобального информационного мониторинга, распространения информации и новых информационных технологий;

деятельность иностранных разведывательных и специальных служб;

преступные действия международных групп, формирований и отдельных лиц, промышленный и банковский шпионаж;

стихийные бедствия и катастрофы;

деятельность международных террористических и экстремистских организаций;

деятельность иностранных политических и экономических структур, направленная против интересов Республики Казахстан.

Внутренними угрозами являются:

противозаконная деятельность политических и экономических структур в области формирования, распространения и использования информации;

неправомерные действия государственных структур, приводящие к нарушению законных прав и интересов физических и юридических лиц, государства в информационной сфере;

нарушения установленных регламентов сбора, обработки, хранения и передачи информации;

преднамеренные неправомерные действия и непреднамеренные ошибки персонала информационных систем;

отказы технических средств и сбои программного обеспечения в информационных и телекоммуникационных системах.

Реализация вышеперечисленных угроз может осуществляться различными способами: информационными, программно-математическими, физическими, радиотехническими и организационно-правовыми.

К информационным способам относятся:

нарушения адресности и своевременности информационного обмена, противозаконный сбор и использование информации;

несанкционированный доступ к информации и информационным ресурсам, неправомерное уничтожение, модификация и копирование данных в информационной сфере;

несанкционированное воздействие и/или манипулирование информацией (дезинформации, сокрытие или искажение информации);

незаконное копирование данных в информационных системах;

использование средств массовой информации с позиций, противоречащих интересам человека, общества и государства;

хищение информации из библиотек, архивов, банков и баз данных;

нарушение технологии обработки информации.

Программно-математические способы включают:

внедрение программ-вирусов;

установку программных и аппаратных закладных устройств;

уничтожение и модификацию данных в информационных системах.

Физические способы включают:

уничтожение или разрушение средств обработки информации и связи;

уничтожение, разрушение или хищение машинных или других оригиналов

носителей информации;

хищение программных или аппаратных ключей и средств криптографической защиты информации;

воздействие на персонал.

Радиотехническими способами являются:

перехват информации с использованием технических средств, размещаемых вблизи объекта защиты либо подключаемых к каналам связи или техническим средствам обработки информации;

электронные устройства перехвата информации в технических средствах и помещениях;

перехват, дешифрование и навязывание ложной информации в сетях передачи данных и линиях связи;

воздействие на парольно-ключевые системы;

радиоэлектронное подавление линий связи и систем управления.

Организационно-правовые способы включают:

закупки несовершенных или устаревших и не прошедших подтверждение соответствия технических средств и средств информатизации;

невыполнение требований законодательства и создание препятствий в принятии необходимых нормативных правовых актов в информационной сфере;

умышленное или безответственное предоставление потребителям недостоверной, неполной, искаженной информации;

неправомерное ограничение доступа к документам, содержащим важную для физических и юридических лиц информацию.

Методы и средства обеспечения информационной безопасности являются общими для различных сфер деятельности государства и группируются следующим образом:

1) правовые: разработка комплекса нормативных правовых актов, регламентирующих информационные отношения в обществе, руководящих и нормативно-методических документов по обеспечению информационной безопасности;

2) программно-технические:

предотвращение утечки за счет побочных электромагнитных излучений и наводок обрабатываемой информации путем исключения несанкционированного доступа или воздействия на нее;

предотвращение специального воздействия, вызывающего разрушение, уничтожение, искажение информации или сбои в работе средств информатизации;

выявление внедренных программных или аппаратных закладных устройств;

специальная защита технических средств обработки информации от средств

технической разведки;

применение криптографических методов и средств защиты информации;

3) организационно экономические:

формирование и обеспечение функционирования систем защиты секретной и конфиденциальной информации;

лицензирование деятельности в сфере информационной безопасности;

техническое регулирование и области информационной безопасности;

контроль и мотивация действий персонала в защищенных информационных системах (экономическое стимулирование, психологическая поддержка и другие);

обеспечение охраны и режима доступа к информационным системам и информационным ресурсам;

проведение социологических исследований (мониторинга) по изучению общественного мнения населения, источников угроз, условий и факторов, влияющих на их возникновение.

Вместе с тем в каждой из сфер деятельности государства, физических и юридических лиц имеются свои особенности обеспечения информационной безопасности, что в первую очередь связано со спецификой решения поставленных задач, наличием свойственных каждой области информационной безопасности слабых элементов и уязвимых звеньев.

Поэтому для каждой сферы требуются специальная организация работ, использование форм и способов обеспечения информационной безопасности с учетом специфических факторов, влияющих на ее состояние.

Основными направлениями обеспечения информационной безопасности являются:

совершенствование нормативной правовой базы, разработка методических и технических документов;

разработка и совершенствование единой политики в области защиты информации;

обеспечение защиты государственных секретов;

противодействие техническим разведкам;

защита от воздействия информационного оружия;

организационно-техническая защита информационных ресурсов, информационно-телекоммуникационных систем и информационной инфраструктуры;

соответствие информационных систем и объектов информатизации требованиям стандартов и нормативных правовых актов в области информации и защиты информации;

подтверждение соответствия технических средств требованиям

информационной безопасности;

выявление, оценка и прогнозирование источников угроз информационной безопасности, оперативное принятие адекватных мер противодействия средствам технической разведки;

научно-техническое обеспечение и научно-исследовательская деятельность по направлениям защиты информации и обеспечению информационной безопасности;

подготовка кадров в области информационных технологий и защиты информации;

международное сотрудничество.

В политической сфере

Объектами обеспечения информационной безопасности в политической сфере являются:

общественное сознание и политическая ориентация различных категорий населения, формируемые под воздействием отечественных и зарубежных средств массовой информации;

система принятия политических решений, во многом зависимая от качества и своевременности ее информационного обеспечения;

система информирования государственными органами населения об общественно-политических и социально-экономических аспектах жизни страны и формирования общественного мнения;

система участия политических партий и общественных организаций в пропаганде своих взглядов в средствах массовой информации.

Угрозу объектам обеспечения информационной безопасности в политической сфере на современном этапе представляют:

государственная или негосударственная монополизация средств массовой информации, а также политическое или экономическое давление на них со стороны отдельных групп, в том числе криминальных;

негативное пропагандистское и психологическое воздействие на общество отечественных и зарубежных средств массовой информации, разжигающих в угоду отдельным политическим силам социальную, межнациональную, межконфессиональную и родовую рознь, противопоставляющих различные категории населения руководству страны;

несовершенство действующего законодательства в области взаимоотношений государства и средств массовой информации;

политизация системы формирования общественного мнения, использование результатов деятельности различных социологических структур, проводящих

опросы населения, в фальсификации или предвзятой интерпретации полученной и м и и н ф о р м а ц и и ;

к о м п ь ю т е р н ы е п р е с т у п л е н и я .

Основными методами обеспечения информационной безопасности в п о л и т и ч е с к о й с ф е р е м о г у т б ы т ь :

постоянное совершенствование законодательства, определяющего правовые и организационные механизмы, регулирующие взаимоотношения субъектов политической жизни в информационной сфере;

обеспечение на базе представительных органов системы независимого и гласного контроля за деятельностью государственных средств массовой информации, социологических и политологических центров, институтов и служб ;

формирование единого информационного пространства Казахстана;

сбалансированное развитие информационного рынка страны;

повышение качества и конкурентоспособности отечественных средств м а с с о в о й и н ф о р м а ц и и ;

содействие постепенному снижению внешнего информационного воздействия, регламентация деятельности зарубежных средств массовой и н ф о р м а ц и и н а т е р р и т о р и и р е с п у б л и к и ;

эффективное реагирование правоохранительными органами и другими государственными органами (прокуратурой, органами финансовой полиции и внутренних дел, уполномоченным органом в области средств массовой информации, местными исполнительными органами областей (города республиканского значения, столицы) на факты нарушения средствами массовой и н ф о р м а ц и и з а к о н о д а т е л ь с т в а ;

создание условий по современной модернизации и совершенствованию имеющихся технических средств и информационных каналов, постоянное изучение зарубежного передового опыта в данной области;

создание системы активной контрпропагиндистской деятельности на информационном и дипломатическом уровнях для предотвращения вмешательства во внутренние дела страны.

В сфере экономики

Среди объектов сферы экономики наиболее подвержены воздействию угроз и н ф о р м а ц и о н н о й б е з о п а с н о с т и :

система государственного управления и статистики;

источники информации о коммерческой деятельности хозяйствующих с у б ъ е к т о в в с е х ф о р м с о б с т в е н н о с т и ;

системы сбора, передачи, хранения и обработки финансовой, биржевой, налоговой, таможенной информации, информации о внешнеэкономической деятельности государства и коммерческих структур, научно-технической информации.

Информационно-вычислительная система государственной статистической отчетности будет обладать достаточной защищенностью от несанкционированного доступа к ее информационным ресурсам. При этом особое внимание будет уделяться защите первичных источников информации и некоторых обобщенных данных, несанкционированное использование которых может нанести ущерб интересам национальной безопасности.

Нормальное функционирование хозяйствующих субъектов нарушается из-за отсутствия нормативных правовых актов, определяющих ответственность источников информации о коммерческой деятельности за недостоверность и сокрытие сведений (о результатах реальной хозяйственной деятельности, об инвестициях и других). С другой стороны, существенный экономический ущерб может быть нанесен государственным и предпринимательским структурам вследствие разглашения (утечки) информации, подлежащей защите.

В системах сбора, передачи, хранения и обработки финансовой, биржевой, налоговой, таможенной информации наибольшую опасность с точки зрения информационной безопасности представляют хищения и преднамеренное искажение информации. Их возможность связана с преднамеренным или случайным нарушением технологии работы с информацией, несанкционированным доступом к ней, что обусловлено недостаточными мерами защиты информации. Аналогичная угроза существует в органах, занятых формированием и распространением информации о внешне экономической деятельности (центральный аппарат министерств, торговые представительства, таможни и другие).

Серьезную опасность для нормального функционирования сферы экономики в целом представляют все более изощренные компьютерные преступления (подлоги, хищения и другие), связанные с проникновением криминальных элементов в компьютерные системы и сети.

Наряду с широким использованием стандартных методов и средств для сферы экономики приоритетными направлениями обеспечения информационной безопасности являются:

разработка и принятие правовых норм, устанавливающих ответственность физических и юридических лиц за несанкционированный доступ и хищение информации, разрушение и искажение информации, преднамеренное распространение недостоверной информации, разглашение информации ограниченного доступа;

повышение достоверности, полноты, сопоставимости и защищенности информации путем введения ответственности первичных источников информации, организации действенного контроля за деятельностью служб обработки и анализа информации, использования специальных организационных и программно-технических средств технической защиты информации;

создание и совершенствование специальной защиты финансовой и коммерческой информации, а также информации персонального характера, касающейся состояния здоровья человека;

разработка комплекса организационно-технических мероприятий по совершенствованию технологии информационной деятельности и защиты информации в хозяйственных, финансовых, промышленных и других экономических структурах с учетом специфической деятельности в сфере экономики;

совершенствование системы профессионального отбора и подготовки персонала для сбора, обработки, анализа и распространения экономической информации.

В оборонной сфере

К объектам информационной безопасности в оборонной сфере, наиболее уязвимым со стороны всего комплекса угроз, относятся:

информационные ресурсы органов военного управления, соединений, частей и учреждений Вооруженных Сил, других войск и воинских формирований Республики Казахстан, содержащие сведения и данные об оперативных и стратегических планах подготовки и ведения боевых действий, о составе и дислокации войск, мобилизационной готовности, тактико-технические данные и характеристики вооружения и военной техники;

информационные ресурсы предприятий оборонного комплекса, содержащие сведения и данные об их научно-техническом и производственном потенциале, объемах поставок и запасах стратегических видов сырья и материалов, основных направлениях развития вооружения, военной техники, их боевых возможностях и о проводимых в интересах обороны фундаментальных и прикладных научно-исследовательских и опытно-конструкторских работах;

системы связи и автоматизированные системы управления войсками и оружием, их информационное обеспечение;

морально-психологическое состояние войск в части, зависящей от информационно-пропагандистского воздействия;

информационная инфраструктура, в том числе центры обработки, анализа и хранения информации органов военного управления, соединений, частей и

учреждений Вооруженных Сил, других войск и воинских формирований Республики Казахстан;

вооружение и военная техника.

Из внешних источником угроз в наибольшей степени способны воздействовать на информационную безопасность объектов оборонной сферы следующие:

все виды разведывательной деятельности иностранных спецслужб и организаций зарубежных государств;

информационно-техническое воздействие (методы радиоэлектронной борьбы, проникновение в компьютерные сети и другие);

психологические операции, осуществляемые специальными методами и через деятельность средств массовой информации;

деятельность иностранных политических и экономических структур, направленная против интересов Республики Казахстан в оборонной сфере;

информационные войны, компьютерные преступления.

Из внутренних источников угроз наибольшую опасность представляют:

нарушение установленных регламентов сбора, обработки и передачи информации в органах военного управления, соединениях, частях и учреждениях Вооруженных Сил, других войск и воинских формирований Республики Казахстан;

преднамеренные действия и непреднамеренные ошибки персонала информационных систем специального назначения;

отказы технических средств и сбои программного обеспечения в информационных и телекоммуникационных системах специального назначения;

информационно-пропагандистская деятельность организаций и отдельных лиц, направленная против интересов государства, подрывающая престиж Вооруженных Сил и их боеготовность.

Эти источники угроз представляют особую опасность в условиях обострения военно-политической обстановки.

Основными направлениями совершенствования информационной безопасности в оборонной сфере являются:

концептуальное, включающее структуризацию целей обеспечения информационной безопасности в оборонной сфере и определяемых ими практических задач;

организационное, связанное с необходимостью формирования оптимальной структуры и состава функциональных органов системы информационной безопасности в оборонной сфере и координации их эффективного взаимодействия, совершенствования приемов и способов стратегической и оперативной маскировки и дезинформации, разведки и радиоэлектронной

борьбы, методов и средств активного противодействия информационно-пропагандистским и психологическим операциям;

техническое, характеризуемое постоянным совершенствованием средств защиты информационных ресурсов от несанкционированного доступа к ним, развитием защищенных систем, в том числе систем связи и управления войсками и оружием, повышением надежности специального программного обеспечения.

Кроме того, одним из главных направлений совершенствования информационной безопасности в оборонной сфере является повышение эффективности защиты информации о разработках, производстве и тактико-технических характеристиках вооружения и военной техники.

В условиях чрезвычайных ситуаций

Наиболее уязвимыми для угроз информационной безопасности в условиях чрезвычайных ситуаций (далее - ЧС) являются система принятия решений по оперативным действиям (реакциям) на их развитие и ход ликвидации последствий, а также система сбора и обработки информации и оповещения о возможном возникновении ЧС.

Особое значение для нормального функционирования этих систем и пунктов управления гражданской обороны имеет защита от повреждений и разрушений информационной инфраструктуры (центров сбора и анализа информации, систем оповещения, систем телекоммуникаций и каналов связи) вследствие аварий, катастроф и стихийных бедствий.

Особенностью информационного воздействия в условиях ЧС является приведение в движение больших масс людей, испытывающих психический стресс, быстрое распространение панических слухов, ложной или недостоверной информации. Нередко в условиях ЧС имеет место сокрытие информации, приводящее к сложностям при ликвидации их последствий.

К специфическим для данной сферы направлениям обеспечения информационной безопасности относятся:

разработка эффективных систем автоматизированного мониторинга признаков предвестников ЧС и оповещения о ЧС и гражданской обороне;

повышение надежности средств обработки и передачи информации, обеспечивающих деятельность центров принятия решений по ЧС, возможность их длительной работы в автономном режиме;

анализ поведения больших масс людей под воздействием ложной или достоверной информации и выработка мер по управлению ими в условиях ЧС;

разработка специальных мер повышения информированности и оповещения населения в условиях ЧС и гражданской обороны;

создание мобильных комплексов, оснащенных средствами обработки и передачи информации, а также средствами для проведения работ в автономном режиме в условиях ЧС.

В общегосударственных информационных и телекоммуникационных системах

Основными объектами обеспечения информационной безопасности в общегосударственных информационных и телекоммуникационных системах являются:

информационные системы государственного и рыночного управления и информационные ресурсы, содержащие сведения, отнесенные к государственным секретам, и конфиденциальную информацию, представленные в виде документированных информационных массивов и баз данных;

средства и системы информатизации (средства вычислительной техники, информационно-вычислительные комплексы, сети и системы), программные средства (операционные системы, системы управления базами данных, другое общесистемное и прикладное программное обеспечение), автоматизированные системы управления, системы связи и передачи данных, технические средства приема, передачи и обработки информации, используемые для обработки информации с ограниченным доступом, их информативные физические поля;

технические средства и системы, не образующие информацию, но устанавливаемые в помещениях, где обрабатывается информация, содержащая сведения, отнесенные к государственным секретам, а также помещения, выделенные для секретных переговоров и проведения секретных работ;

государственные информационные ресурсы, содержащие сведения, составляющие государственные секреты;

информационные ресурсы органов военного управления, национальной безопасности, внутренних дел, содержащие сведения об оперативных и стратегических планах подготовки и ведения боевых действий, об их численном и кадровом составах, направлениях деятельности, мобилизационной готовности, системах связи и управления войсками и оружием, их информационном обеспечении, информационной инфраструктуре;

режимные и стратегические объекты, объекты средств вычислительной техники, на которых обрабатывается информация ограниченного доступа;

информационная инфраструктура "электронного правительства".

Основными направлениями обеспечения информационной безопасности в общегосударственных информационных и телекоммуникационных системах являются:

обеспечение бесперебойного функционирования информационных систем органов государственного управления;

специальная защита информации от средств технической разведки;

исключение несанкционированного доступа к обрабатываемой или хранящейся в технических средствах информации;

предотвращение утечки обрабатываемой информации за счет побочных электромагнитных излучений и наводок на объектах средств вычислительной техники;

предотвращение программно-технического воздействия, вызывающего разрушение, уничтожение, искажение информации или сбои в работе средств информатизации;

выявление внедренных на объекты и в технические средства электронных устройств перехвата информации (закладных устройств);

предотвращение перехвата техническими средствами речевой информации из помещений и объектов.

Предотвращение перехвата с помощью технических средств информации, передаваемой по каналам связи, достигается применением криптографических и иных методов и средств защиты, а также проведением необходимых организационно-технических мероприятий.

Исключение несанкционированного доступа и воздействия передаваемой, обрабатываемой или хранящейся в технических средствах информации достигается применением специальных программно-технических средств защиты, использованием криптографических способов защиты, а также организационными и режимными мероприятиями.

Предотвращение утечки обрабатываемой информации за счет побочных электромагнитных излучений и наводок, а также электроакустических преобразований достигается применением защищенных технических средств, технических средств защиты, в том числе средств криптографической защиты информации, средств активной защиты, экранированием объектов, установлением контролируемой (проверяемой) зоны вокруг объектов защиты и другими организационными и техническими мерами.

Предотвращение программно-технического воздействия, вызывающего разрушение, уничтожение, искажение информации или сбои в работе средств информатизации, достигается применением лицензионного программного обеспечения, специальных программных и аппаратных средств защиты (антивирусные процессоры, антивирусные программы), организацией системы контроля безопасности программного обеспечения.

Выявление внедренных на объекты и в технические средства электронных устройств перехвата информации (закладных устройств) достигается

проведением специальных исследований.

Предотвращение перехвата техническими средствами речевой информации из помещений и объектов достигается за счет применения технических средств защиты, проектных и конструкторских решений, обеспечивающих звукоизоляцию помещений, проведения специальных обследований режимных помещений по выявлению и деактивизации установленных средств перехвата и других организационных и режимных мероприятий.

Основными организационно-техническими мероприятиями по защите информации в общегосударственных информационных и телекоммуникационных системах являются:

лицензирование деятельности организаций в области технической защиты информации;

создание разрешительной системы допуска и доступа физических и юридических лиц к государственным секретам;

аттестация объектов информатизации по выполнению требований обеспечения информационной безопасности;

подтверждение соответствия требованиям информационной безопасности технических средств защиты информации и контроль за ее эффективностью, средств информатизации и связи;

создание и применение информационных и автоматизированных систем управления в защищенном исполнении;

разработка и использование технических средств защиты информации и методов контроля за ее эффективностью;

применение методов, технических мер и технических средств защиты, в том числе средств криптографической защиты информации, исключающих перехват информации, передаваемой по каналам связи;

организация защиты информации от несанкционированного доступа и воздействия, от заражения компьютерными вирусами в информационно-телекоммуникационных системах и локальных вычислительных сетях;

разработка мер по предотвращению утечки обрабатываемой информации за счет побочных электромагнитных излучений и наводок на объектах средств вычислительной техники;

проведение мероприятий, включающих в себя реализацию организационных и инженерно-технических мер по обеспечению функционирования систем охраны объектов, предусматривающих несколько рубежей охраны, с комплексным применением интегрированных систем охраны, видеонаблюдения, сбора и обработки информации для осуществления надежной охраны и обнаружения фактов несанкционированного проникновения в охраняемую зону

о б ъ е к т а ;

проведение контроля эффективности защищенности объектов от утечки информации за счет побочных электромагнитных излучений и наводок;

специальные обследования режимных помещений по выявлению внедренных на объекты и в технические средства электронных устройств перехвата информации (закладных устройств);

проведение контроля эффективности защищенности локальных вычислительных сетей от несанкционированного доступа к информации;

организация, координация и финансирование научно-исследовательских и опытно-конструкторских работ в области обеспечения информационной б е з о п а с н о с т и ;

разработка технических решений в целях перспективного развития в сфере обеспечения информационной безопасности и совершенствования сетей телекоммуникаций специального назначения;

выявление, оценка и прогнозирование источников угроз информационной безопасности, оперативное принятие адекватных мер противодействия техническим средствам разведки;

сбор информации о технических разведках, их устремлениях, возможностях, методах их работы и техническом оснащении;

расширение межгосударственного сотрудничества в рамках заключенных договоренностей между государствами, направленного на обмен опытом по проблемам борьбы с преступлениями в области информационной безопасности;

контрразведывательные мероприятия, направленные на получение информации о предпринимаемых действиях источников информационных угроз против Республики Казахстан;

создание учебно-методической и материальной базы подготовки специалистом в области обеспечения информационной безопасности;

обеспечение режима секретности и защиты информации, укрепление собственной безопасности государственных органов и организаций.

Конкретные методы, приемы и меры защиты информации разрабатываются в зависимости от степени возможного ущерба в случаях утечки, разрушения или уничтожения.

В области науки и техники

Наиболее уязвимыми объектами информационной безопасности в области науки и техники являются:

результаты фундаментальных, поисковых и прикладных научных исследований, содержащие сведения, данные и знания, потенциально важные для

научно-технического, технологического и социально-экономического развития страны, утрата которых может нанести ущерб национальным интересам Республики Казахстан;

незапатентованные технологии, ноу-хау, промышленные образцы модели и экспериментальное оборудование, для которых еще не определили статус конфиденциальности и которые поэтому не подпадают под законодательство Республики Казахстан и могут быть проданы за рубеж;

объекты интеллектуальной собственности (открытия, патенты изобретения, промышленные образцы, программные продукты и другие), которые могут быть похищены и незаконно распространены или использованы несмотря на их правовую защиту.

При классификации угроз в этой области необходимо уделять особое внимание изучению возможности промышленного шпионажа специальных служб иностранных государств и криминальных структур.

Будет организована система оценки возможных последствий воздействия угроз на указанные объекты, включающая общественные научные советы и институт независимых экспертиз, вырабатывающие рекомендации для каждого конкретного случая распространения или научной, технической и технологической продукции, с целью предотвращения незаконного присвоения или использования научного и интеллектуального потенциала.

Со стороны государства реальный путь противодействия угрозам заключается в постоянном совершенствовании законодательства в этой области и механизмов его реализации. Многие мероприятия по предотвращению или нейтрализации угроз в этой области, особенно в части, касающейся научных кадров, относятся к сфере социальной и экономической политики государства.

В сфере духовной жизни и информационной безопасности личности

Объектами обеспечения информационной безопасности в сфере духовной жизни являются:

мировоззрение людей, их жизненные ценности и идеалы, в частности такие важные для государства и общества, как патриотизм, гражданский долг, этническая и религиозная терпимость и тому подобные;

социальная и личностная ориентация личности;

культурные и эстетические запросы, во многом определяющие мировоззрение людей;

психическое здоровье личности.

Сфера духовной жизни как ни одна другая чувствительна к

информационно-пропагандистскому воздействию, идеологическому давлению, культурной экспансии, осуществляемым преимущественно через средства массовой информации.

В этой связи средства массовой информации играют определяющую роль в формировании духовной жизни личности, что обусловливает их особую ответственность перед обществом. Особое место при этом занимает Интернет, который ввиду его открытости и доступности может использоваться в интересах международного терроризма как средство воздействия на личность негативной информацией, призывающей к насилию, межнациональной розни, религиозному экстремизму.

Предотвращение и нейтрализация угроз информационной безопасности в сфере духовной жизни требуют, прежде всего, государственной идеологии, приемлемой для большинства населения и учитывающей интересы, культурные и исторические традиций многочисленных этносов, населяющих страну. На основе такой идеологии могут быть выработаны четкие критерии оценки угроз информационной безопасности, основные приоритеты и государственная политика в этой сфере.

Наряду с этим требуются цивилизованные, демократические формы и методы взаимодействия со средствами массовой информации в целях привлечения к формированию и распространению духовных ценностей, отвечающих национальным интересам страны, защите их от враждебной или недружественной пропаганды.

Требуются законодательное регулирование сферы Интернета, реализация организационно-правовых мер с целью контроля трафика на наличие вредоносной и негативной информации.

Необходима разработка правовых и организационных мер, препятствующих коммерциализации культуры и обеспечивающих сохранение и развитие информационных ресурсов, составляющих историко-культурное наследие.

В области международного сотрудничества

Международное сотрудничество в области информационной безопасности (далее - сотрудничество) есть неотъемлемая составляющая политического, военного, экономического, культурного и других видов взаимодействия стран - участниц мирового сообщества.

Основными направлениями сотрудничества, отвечающими интересам Республики Казахстан, являются:

обеспечение информационной безопасности трансграничного информационного обмена и регламента обмена, а также сохранности и

неискаженное информации при ее передаче по телекоммуникационным каналам;

координация деятельности государств-участников международного сотрудничества по предотвращению компьютерных преступлений;

предотвращение несанкционированного доступа к защищаемой информации в международных банковских сетях и каналах информационного обеспечения мировой торговли, к защищаемой информации в международных политических, экономических и военных союзах, блоках и организациях, к информации в международных правоохранительных организациях, ведущих борьбу с международной организованной преступностью, международным терроризмом, распространением наркотиков и незаконной торговлей оружием и радиоактивными материалами;

создание совместных международных проектов по разработке новых систем информационного обмена, совершенствованию технологической базы и формированию информационных систем и систем безопасности информационных ресурсов.

Особое внимание будет уделено сотрудничеству со странами Содружества Независимых Государств, государствами-членами Евразийского экономического сообщества, Организации Договора о коллективной безопасности, Шанхайской организации сотрудничества.

Для реализации указанных направлений сотрудничества необходимы:

активное участие Казахстана в международных организациях, действующих в области обеспечения информационной безопасности;

обмен опытом в области обеспечения информационной безопасности, в том числе через международные и отечественные издания.

На основе изложенных принципов и положений определяются приоритетные направления формирования и реализации политики информационной безопасности в политической, военной, экономической и других сферах деятельности государства.

Государственная политика в сфере информационной безопасности предусматривает согласование интересов субъектов информационных отношений, организацию эффективной работы государственных органов и организаций с широким представительством общественных и неправительственных организаций.