Концепция информационной безопасности Российской Федерации

ПРОЕКТ

Совет безопасности Российской Федерации

Межведомственная комиссия по информационной безопасности

КОНЦЕПЦИЯ

информационной безопасности Российской Федерации

АННОТАЦИЯ

В Концепции информационной безопасности Российской Федерации (далее — Концепция) на основе анализа современного состояния информационной безопасности определены цели, задачи и ключевые проблемы обеспечения информационной безопасности.

Рассмотрены объекты, угрозы информационной безопасности и возможные их последствия, методы и средства предотвращения, парирования и нейтрализации угроз, а также особенности обеспечения информационной безопасности в различных сферах деятельности государства.

Излагаются основные положения государственной политики обеспечения информационной безопасности в Российской Федерации, организационная структура и принципы построения системы информационной безопасности.

Концепция служит методологической основой разработки комплекса нормативно-правовых и организационно-методических документов, регламентирующих деятельность в области информационной безопасности органов представительной, исполнительной и судебной властей Российской Федерации, субъектов Российской Федерации, органов местного самоуправления (далее — органы государственной власти и управления), предприятий, учреждений и организаций независимо от их организационно-правовой формы и формы собственности (далее — предприятия).

I. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Назначение, правовая основа Концепции информационной безопасности Российской Федерации

Концепция информационной безопасности Российской Федерации представляет собой официально принятую систему взглядов на проблему обеспечения информационной безопасности, методы и средства защиты жизненно важных интересов личности, общества, государства в информационной сфере.

Концепция является составной частью Концепции национальной безопасности Российской Федерации и служит методологической основой:

разработки стратегии обеспечения информационной безопасности страны, включающей в себя цели, задачи и комплекс основных мер по ее практической реализации;

формирования и проведения государственной политики Российской Федерации в области обеспечения информационной безопасности;

подготовки предложений по совершенствованию правового, нормативно-методического, научно-технического и организационного обеспечения информационной безопасности Российской Федерации;

разработки целевых программ защиты информационных ресурсов и средств информатизации.

Положения Концепции должны учитываться при формировании государственной политики информатизации, создания и развития единого информационного пространства России.

Правовую основу Концепции составляют Конституция Российской Федерации, законы Российской Федерации "О безопасности", "О государственной тайне", "Об информации, информатизации и защите информации", другие законодательные акты Российской Федерации, а также международные договоры и соглашения, заключенные или признанные Российской Федерацией, определяющие права и ответственность граждан, общества и государства в информационной сфере.

1.2. Роль и место информационной безопасности в общей системе национальной безопасности Российской Федерации

Информационная безопасность играет ключевую роль в обеспечении Жизненно важных интересов Российской Федерации. Это, в первую очередь, обусловлено насущной потребностью, создания развитой и защищенной информационной среды общества. Именно через информационную среду осуществляются угрозы национальной безопасности в различных сферах деятельности государства.

В политической сфере все большее значение приобретают информационные факторы. В традиционном противостоянии политических соперников растут удельный вес и значимость информационно-психологического воздействия.

Экономический потенциал государства все в большей степени определяется объемом информационных ресурсов и уровнем развития информационной инфраструктуры. В то же время растет уязвимость экономических структур от недостоверности, запаздывания и незаконного использования экономической информации.

В военной сфере исход вооружённой борьбы все в большей степени зависит от качества добываемой информации и уровня развития информационных технологий, на которых основываются системы разведки, радиоэлектронной борьбы, управления войсками и высокоточным оружием.

В сфере духовной жизни возникает опасность развития в обществе агрессивной потребительской идеологии, тотальной коммерциализации культуры, распространения идей насилия и нетерпимости, воздействия на психику разрушительных форм мифологизированного сознания. Эти угрозы и защита от них, а также утверждение нравственных ценностей реализуются внутри информационной среды и прежде всего через средства массовой информации и формирования общественного мнения.

Информационная среда, являясь системообразующим фактором во всех сферах национальной безопасности, активно влияет на состояние политической, экономической, оборонной и других составляющих национальной безопасности Российской Федерации. В то же время она представляет собой самостоятельную сферу национальной безопасности, в которой необходимо обеспечить защиту информационных ресурсов, систем их формирования, распространения и использования, информационной инфраструктуры, реализацию прав на информацию государства, юридических лиц, граждан.

1.3. Основные цели и задачи обеспечения информационной безопасности Российской Федерации

Основные цели обеспечения информационной безопасности определяются на базе устойчивых приоритетов национальной безопасности, отвечающих долговременным интересам общественного развития, к которым относятся:

сохранение и укрепление российской государственности и политической стабильности в обществе;

сохранение и развитие демократических институтов общества, обеспечение прав и свобод граждан, укрепление законности и правопорядка;

обеспечение достойной роли России в мировом сообществе;

обеспечение территориальной целостности страны;

обеспечение прогрессивного социально-экономического развития России;

сохранение национальных культурных ценностей и традиций.

В соответствии с указанными приоритетами основными целями информационной безопасности являются:

защита национальных интересов России в условиях глобализации информационных процессов, формирования мировых информационных сетей и стремления США и других развитых стран к информационному доминированию;

обеспечение органов государственной власти и управления, предприятий и граждан достоверной, полной и своевременной информацией, необходимой для принятия решений, а также предотвращение нарушений целостности и незаконного использования информационных ресурсов;

реализация прав граждан, организаций и государства на получение, распространение и использование информации.

К основным задачам обеспечения информационной безопасности относятся:

выявление, оценка и прогнозирование источников угроз информационной безопасности;

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

разработка нормативно-правовой базы обеспечения информационной безопасности, координация деятельности органов государственной власти и управления и предприятий по обеспечению информационной безопасности;

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

обеспечение активного участия России в процессах создания и использования глобальных информационных сетей и систем.

1.4. Объекты информационной безопасности Российской Федерации

К объектам информационной безопасности Российской Федерации относятся:

информационные ресурсы, вне зависимости от форм хранения, содержащие информацию, составляющую государственную тайну и ограниченного доступа,

коммерческую тайну и другую конфиденциальную информацию, а также открытую (общедоступную) информацию и знания;

система формирования, 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;

информационная инфраструктура, включающая центры обработки и анализа информации, каналы информационного обмена и телекоммуникации, механизмы обеспечения функционирования телекоммуникационных систем и сетей, в том числе системы и средства защиты информации;

система формирования общественного сознания (мировоззрение, политические взгляды, моральные ценности и пр.), базирующаяся на средствах массовой информацией пропаганды;

права граждан, юридических лиц и государства на получение, распространение и использование информации, защиту конфиденциальной информации и интеллектуальной собственности.

Информационная безопасность всех вышеуказанных объектов создает условия надежного функционирования государственных и общественных институтов, а также формирования общественного сознания, отвечающего прогрессивному развитию страны.

II. АНАЛИЗ СОСТОЯНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ

2.1. Основные факторы, влияющие на состояние информационной безопасности Российской Федерации

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

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

Политическими факторами являются:

изменение геополитической обстановки вследствие фундаментальных перемен в различных регионах мира, сведения к минимуму вероятности мировой ядерной и обычной войн;

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

становление новой российской государственности на основе принципов демократии, законности, информационной открытости;

разрушение ранее существовавшей командно-административной системы государственного управления, а также сложившейся системы обеспечения безопасности страны;

нарушение информационных связей вследствие образования независимых государств на территории бывшего СССР;

стремление России к более тесному сотрудничеству с зарубежными странами в процессе проведения реформ на основе максимальной открытости сторон;

низкая общая правовая и информационная культура в российском обществе.

Среди экономических факторов наиболее существенными являются: переход России на рыночные отношения в экономике, появление множества отечественных и зарубежных коммерческих структур — производителей и потребителей информации, средств информатизации и защиты информации, включение информационной продукции в систему товарных отношений;

критическое состояние отечественных отраслей промышленности, производящих средства информатизации и защиты информации;

расширяющаяся кооперация с зарубежными странами в развитии информационной инфраструктуры России.

Из организационно-технических факторов определяющими являются:

недостаточная нормативно-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 России;

широкое использование в сфере государственного управления и кредитно-финансовой сфере незащищенных от утечки информации импортных технических и программных средств для хранения, обработки и передачи информации;

рост объемов информации, передаваемой по открытым каналам связи, в том числе по сетям передачи данных и межмашинного обмена;

обострение криминогенной обстановки, рост числа компьютерных преступлений, особенно в кредитно-финансовой сфере.

2.2. Оценка состояния и ключевые проблемы обеспечения информационной безопасности Российской Федерации

За последние годы в Российской Федерации реализован комплекс практических мер по совершенствованию информационной безопасности.

Начато формирование нормативно-правового обеспечения информационной безопасности. Приняты законы Российской Федерации "О государственной тайне", "Об информации, информатизации и защите информации", развернуты работы по созданию механизмов их реализации, завершена подготовка ряда законопроектов, регламентирующих деятельность \S субъектов в информационной сфере. Осуществлен ряд практических мероприятий по совершенствованию информационной безопасности в органах государственной власти и управления и на предприятиях. Успешному решению ряда вопросов информационной безопасности способствует создание Государственной системы защиты информации и системы лицензирования деятельности предприятий в области защиты информации.

Вместе с тем, анализ современного состояния информационной безопасности в России показывает, что уровень информационной безопасности в настоящее время не соответствует жизненно важным потребностям личности, общества и государства.

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

Отсутствие действенных механизмов регулирования информационных отношений в обществе и государстве приводит ко многим негативным последствиям.

Слабое обеспечение органов государственной власти и управления полной, достоверной и своевременной информацией затрудняет принятие обоснованных решений. Неразвитость информационных отношений в сфере предпринимательства тормозит становление цивилизованного рынка. Отсутствие механизма включения информационного ресурса в хозяйственный оборот приводит к серьезным экономическим потерям.

Недостаточная защищенность государственного информационного ресурса приводит к утрате важной политической, экономической и научно-технической информации, в том числе о новых и высокоэффективных технологиях военного и двойного назначения.

Необеспеченность прав граждан на информацию, манипулирование информацией вызывает неадекватную реакцию населения и в ряде случаев ведет к политической нестабильности в обществе.

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, слабый контроль за экспортом отечественных наукоемких технологий, образцов вооружения и военной техники.

Неблагоприятно обстоят дела с охраной государственной тайны. Серьезно ослаблены меры по обеспечению сохранности государственных секретов, коммерческой и служебной тайны в органах государственной власти и управления и на предприятиях оборонного комплекса.

Гарантированные Конституцией Российской Федерации основные права и свободы, такие как право на неприкосновенность частной жизни, личную и семейную тайну, тайну переписки, практически не имеют правового, организационного и технического обеспечения. Неудовлетворительно организована защита персональных данных, налоговой, таможенной, имущественной и другой информации.

Продолжается спад производства на государственных предприятиях, в том числе специализирующихся на выпуске защищенной техники, предназначенной для обработки секретной информации. Разрушаются научные и производственные коллективы, наблюдается массовый уход в коммерческие структуры наиболее квалифицированных кадров.

Отставание отечественных информационных технологий вынуждает массового потребителя идти по пути закупок незащищенной импортной техники, в результате чего повышается вероятность несанкционированного доступа к базам и банкам данных, а также возрастает зависимость страны от иностранных производителей компьютерной и телекоммуникационной Техники и информационной продукции.

Такое положение дел в области обеспечения информационной безопасности не позволяет России на равноправной основе включиться в мировую информационную систему и требует безотлагательного решения следующих ключевых проблем:

1. Развития научно-практических основ информационной безопасности, отвечающей современной геополитической ситуации и условиям политического и социально-экономического развития Российской Федерации.

2. Формирования законодательной и нормативно-правовой базы обеспечения информационной безопасности, в том числе разработка реестра

информационного ресурса, регламента информационного обмена для органов государственной власти и управления, предприятий, нормативного закрепления ответственности должностных лиц и граждан за соблюдение требований информационной безопасности.

3. Разработки механизмов реализации прав граждан на информацию.

4. Формирования системы информационной безопасности, обеспечивающей реализацию государственной политики в области информационной безопасности.

5. Разработки современных методов и технических средств, обеспечивающих комплексное решение задач защиты информации.

6. Разработки критериев и методов оценки эффективности систем и средств информационной безопасности и их сертификации.

7. Исследований форм и способов цивилизованного воздействия государства на формирование общественного сознания.

8. Комплексного исследования деятельности персонала информационных систем, в том числе методов повышения мотивации, морально-психологической устойчивости и социальной защищенности людей, работающих с секретной и конфиденциальной информацией.

III. УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ

3.1. Источники угроз информационной безопасности Российской федерации

Источники угроз информационной безопасности в Российской Федерации можно разделить на внешние и внутренние. К внешним источникам относятся:

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

деятельность иностранных разведывательных и специальных служб;

деятельность иностранных политических и экономических структур, направленная против интересов Российского государства;

преступные действия международных групп, формирований и отдельных лиц;

стихийные бедствия и катастрофы. Внутренними источниками угроз являются:

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

неправомерные действия государственных структур, приводящие к Нарушению законных прав граждан и организаций в информационной сфере;

нарушения установленных регламентов сбора, обработки и передачи информации;

преднамеренные действия и непреднамеренные ошибки персонала информационных систем;

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

3.2. Способы воздействия угроз на объекты информационной безопасности Российской Федерации

Способы воздействия угроз на объекты информационной безопасности в Российской Федерации подразделяются на информационные, программно-математические, физические, радиоэлектронные, организационно-правовые.

К информационным способам относятся:

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

несанкционированный доступ к информационным ресурсам;

манипулирование информацией .(дезинформация, сокрытие или искажение информации);

незаконное копирование данных в информационных системах;

использование средств массовой информации с позиций, противоречащих интересам граждан, организаций 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 или 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;

поставка "зараженных" компонентов информационных систем.

Радиоэлектронными способами являются:

перехват информации в технических каналах ее утечки;

внедрение электронных устройств перехвата информации в технических средствах й 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 информационных технологий и средств информатизации;

невыполнение требований законодательства и задержки в принятии необходимых нормативно-правовых положений в информационной сфере;

неправомерное ограничение доступа к документам, содержащим важную для граждан и организаций информацию.

3.3. Возможные последствия воздействия угроз информационной безопасности Российской Федерации

В результате воздействия угроз информационной безопасности может быть нанесен серьезный ущерб жизненно важным интересам Российской Федерации в политической, экономической, оборонной и других сферах деятельности государства, причинен социально-экономический ущерб обществу и отдельным гражданам.

Вследствие такого воздействия могут быть созданы препятствия на пути равноправного сотрудничества России с развитыми странами и дружественными государствами, затруднено принятие важнейших политических, экономических и других решений, подорван государственный

авторитет Российской Федерации на международной арене, создана атмосфера напряженности и политической нестабильности в обществе, нарушен баланс интересов личности, общества и государства, дискредитированы органы государственной власти и управления, спровоцированы социальные, национальные и религиозные конфликты, инициированы забастовки и массовые беспорядки, нарушено функционирование системы государственного управления, а также систем управления войсками, вооружением и военной техникой, объектами повышенной опасности.

Следствием воздействия угроз могут явиться снижение темпов научно-технического развития страны, утрата культурного наследия, проявления бездуховности и безнравственности.

Весьма существенный экономический ущерб в различных областях общественной жизни и в сфере бизнеса может быть причинен в результате нарушений законодательства в информационной сфере и компьютерных преступлений,

Угрозы информационной безопасности могут нанести физический, материальный и моральный ущерб гражданам, вызывать неадекватное социальное и криминальное поведение групп людей или отдельных лиц, оказать влияние на процессы образования и формирования личности.

IV. МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ

4.1. Базовые методы предотвращения, парирования и нейтрализации угроз информационной безопасности Российской Федерации

В целях предотвращения, парирования и нейтрализации угроз информационной безопасности применяются правовые, программно-технические и организационно-экономические методы.

Правовые методы предусматривают разработку комплекса нормативно-правовых актов и положений, регламентирующих информационные отношения в обществе, руководящих и нормативно-методических документов по обеспечению информационной безопасности.

Программно-технические методы включают предотвращение утечки обрабатываемой информации путем исключения несанкционированного доступа К ней, предотвращение специальных воздействий, вызывающих разрушение; уничтожение, искажение информации или сбои в работе средств информатизации, выявление внедренных программных или аппаратных закладных устройств, исключение перехвата информации техническими средствами, применения криптографических средств защиты информации при передаче по каналам связи.

Организационно-экономические методы предусматривают формирование и обеспечение функционирования систем защиты секретной и конфиденциальной информации, сертификации этих систем по требованиям информационной безопасности, лицензирования деятельности в сфере информационной безопасности, стандартизации способов и средств защиты информации, контроль за действием персонала в защищенных информационных системах.

Важное место среди этих методов занимают мотивация; экономическое стимулирование и психологическая поддержка деятельности персонала, занятого обеспечением информационной безопасности.

4.2. Особенности обеспечения информационной безопасности в различных сферах, деятельности государства и общегосударственных информационных и телекоммуникационных системах

Рассмотренные выше объекты, угрозы, методы и средства обеспечения информационной безопасности являются общими для различных сфер деятельности государства.

Вместе с тем, в каждой из этих сфер 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 в каждой сфере деятельности государства требуется специальная организация работ, использование форм и способов обеспечения информационной безопасности с учетом специфических факторов, влияющих на ее состояние.

В политической сфере

Наиболее серьезной опасности в политической сфере подвергаются: общественное сознание и политическая ориентация различных групп населения страны (регионов), непрерывно формируемые под воздействием отечественных и зарубежных средств массовой информации (печать, радио, телевидение);

система принятия политических решений, существенно зависящая от качества и своевременности ее информационного обеспечения;

права политических организаций, партий, объединений и движений на закрепленное в Конституций Российской Федерации свободное выражение своих программ, социально-политических и экономических ориентации через средства массовой информации;

система регулярного информирования населения органами государственной власти и управления о политической и социально-экономической жизни через

средства массовой информации, пресс-центры, центры общественных связей и т.п.;

система формирования общественного мнения, включающая специальные институты, центры и службы выявления, изучения и анализа общественного мнения.

Для демократического развития страны наибольшую опасность представляют следующие угрозы:

односторонняя политическая ориентация средств массовой информации под давлением государственных органов, господствующих политических сил, а также под экономическим давлением отдельных групп, в том числе криминальных структур;

пропагандистское и психологическое воздействие на политическую ориентацию населения зарубежных и отечественных средств массовой информации в интересах отдельных политических сил;

отсутствие или несовершенство законодательства, обязывающего органы государственной власти и управления регулярно и полно информировать население о своей деятельности и состоянии дел в сфере своей компетентности;

препятствия со стороны государства осуществлению законных и равных прав различных политических сил, в том числе оппозиционных, на использование средств массовой информации, контролируемых государством;

политизация системы формирования общественного мнения, ведущая к искажению реальных ситуаций (фальсификация или предвзятая интерпретация результатов опросов или референдумов).

Основными мероприятиями обеспечения информационной безопасности в политической сфере являются:

разработка и постоянное совершенствование законодательства, правовых и организационных механизмов, регулирующих взаимоотношения всех субъектов политической жизни в реализации их конституционных прав и обязанностей в использовании средств массовой информации;

создание системы независимого и гласного контроля за деятельностью государственных средств массовой информации, институтов, центров и служб изучения общественного мнения, а также специальных служб по связи с населением;

активизация контрпропагандистской деятельности и дипломатических усилий по предотвращению информационно-пропагандистского вмешательства во внутренние дела страны.

В сфере экономики

Среди объектов сферы экономики наиболее подвержены воздействию угроз информационной безопасности: система государственной статистики;

источники, порождающие информацию о коммерческой деятельности хозяйственных субъектов всех форм собственности, о потребительских свойствах товаров и услуг;

системы сбора и обработки финансовой, биржевой, налоговой, таможенной информации, информации о внешнеэкономической деятельности государства и коммерческих структур.

Система государственной статистической отчетности должна обладать достаточной защищенностью от серьезных и массовых искажений. Особое внимание должно уделяться защите первичных источников информации и обобщённых отчетных данных.

В конечном итоге информация в системе государственной статистики должна обладать полнотой, достоверностью, достаточностью, сопоставимостью и регулярностью - свойствами, необходимыми для принятия рациональных решений на уровнях государства, отрасли, предприятия, для проведения общеэкономического анализа и прогнозирования развития народного хозяйства.

Нормальное функционирование хозяйственных объектов нарушается из-за отсутствия нормативно-правовых положений, определяющих ответственность источников информации о коммерческой деятельности и потребительских свойствах товаров Н услуг за недостоверность и сокрытие сведений (о результатах реальной хозяйственной деятельности, об инвестициях и др.). С другой стороны, существенный экономический ущерб может быть нанесен Государственным и предпринимательским структурам вследствие разглашения информации, содержащей коммерческую тайну.

В системах сбора и обработки финансовой, биржевой, налоговой, таможенной информации наибольшую опасность с точки зрения информационной безопасности представляют хищения и преднамеренное искажение информации, возможность которых связана с преднамеренным или случайным Нарушением технологии работы с информацией, несанкционированным доступом к ней, что обусловлено недостаточными мерами защиты информации. Такая же опасность существует в органах, занятых формированием и распространением информации о внешнеэкономической деятельности (центральный аппарат ведомств, торгпредства, таможни и т.п.).

Серьезную опасность для Нормального функционирования сферы экономики в целом представляют все более изощренные компьютерные преступления (подлоги, хищения и т.д.), 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 положений, устанавливающих ответственность юридических и физических лиц за несанкционированный доступ и хищение информации, преднамеренное распространение недостоверной информации, разглашение коммерческой тайны, утечку конфиденциальной информации;

коренная перестройка системы государственной статистической отчетности, направленная на повышение достоверности, полноты, сопоставимости и защищенности информации путем введения строгой юридической ответственности первичных источников информации, организации действенного контроля за их деятельностью и деятельностью служб обработки и анализа статистической информации, ограничения ее коммерциализации, использования специальных организационных и программно-технических средств защиты информации;

создание и совершенствование специальных средств Защиты финансовой и коммерческой информации;

разработка комплекса организационно-технических мероприятий по совершенствованию технологии информационной деятельности и защиты информации в хозяйственных, финансовых, промышленных и других экономических структурах с учетом специфических для сферы экономики требований информационной безопасности;

совершенствование системы профессионального отбора и подготовки персонала систем 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 аппарата Министерства обороны, Генерального штаба, главных штабов видов Вооруженных сил и родов войск, научно-исследовательских учреждений, содержащие сведения и данные об оперативных и стратегических планах подготовки и ведения боевых действий, о составе и дислокации войск, о мобилизационной готовности, тактико-технических характеристиках вооружения и военной техники;

информационные ресурсы предприятий оборонного комплекса, содержащие сведения и данные об их научно-техническом и производственном потенциалах, об объемах поставок и запасах стратегических видов сырья и материалов, об основных направлениях развития вооружения, военной техники, их боевых

возможностях и проводимых в интересах обороны фундаментальных и прикладных НИР;

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

политико-моральное состояние войск в части, зависящей от информационно-пропагандистского воздействия;

информационная инфраструктура, в том числе центры обработки и анализа информации Генерального штаба и информационные подразделения штабов видов Вооруженных Сил, штабов объединений и соединений видов Вооруженных Сил и родов войск, пункты управления, узлы и линии радио-, радиорелейной, тропосферной и спутниковой связи, а также линии проводной связи, развертываемые и арендуемые Министерством обороны и другими силовыми структурами.

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

все виды разведывательной деятельности зарубежных государств;

информационно-технические воздействия (методы радиоэлектронной борьбы, проникновение в компьютерные сети и т.п.) со стороны вероятных противников;

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

деятельность иностранных политических и экономических структур, направленная против интересов Российской Федерации в оборонной сфере.

Из внутренних источников угроз наибольшую опасность представляют:

нарушение- установленных регламентов сбора, обработки и передачи информации в штабах и учреждениях Министерства обороны, в организациях и на предприятиях оборонного комплекса;

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.

Главными направлениями совершенствования информационной безопасности в оборонной сфере являются:

концептуальное, включающее структуризацию целей обеспечения информационной безопасности в оборонной сфере, вытекающих из них практических задач, корректное определение информационных угроз и их источников;

техническое, характеризуемое постоянным совершенствованием средств защиты информационных ресурсов от методов и средств несанкционированного доступа к ним, развитием защищенных, засекреченных систем связи и управления войсками и оружием, повышение надежности специального программного обеспечения;

организационное, связанное с необходимостью формирования оптимальной структуры и состава функциональных органов системы информационной безопасности в оборонной сфере и координации их аффективного взаимодействия, совершенствование приемов и способов стратегической и оперативной маскировки, разведки и радиоэлектронной борьбы, методов и средств активного противодействия информационно-пропагандистским и психологическим операциям вероятного противника.

Кроме того, одним из главных направлений совершенствования информационной безопасности в оборонной сфере является повышение эффективности защиты технологий производства и тактико-технических характеристик вооружения и военной техники. 9

В условиях чрезвычайных ситуаций

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

Особое значение для нормального функционирования этих объектов имеет разрушение информационной инфраструктуры (центров сбора и анализа информации, технических средств обработки и передачи информации, систем телекоммуникации и каналов связи) вследствие аварий, катастроф и стихийных бедствий. Эти события, а также задержка, искажение и разрушение оперативной информации, несанкционированный доступ к ней отдельных лиц или групп людей могут привести к тяжелым последствиям.

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 ее последствий.

К специфическим для данной сферы направлениям обеспечения информационной безопасности относятся:

разработка эффективной системы мониторинга признаков — предвестников ЧС;

повышение надежности средств обработки и передачи информации, обеспечивающих деятельность центров принятия решений по ЧС;

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

разработка специальных мер повышения информированности населения в условиях ЧС.

В общегосударственных информационных и телекоммуникационных системах

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

информационные ресурсы, содержащие сведения, отнесенные к государственной тайне, 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 (звукозаписи, звукоусиления, звукосопровождения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки графической, смысловой и буквенно-цифровой информации), используемые для обработки информации ограниченного доступа, их информативные физические поля;

технические средства и системы, не обрабатывающие информацию, но размещенные в помещениях, где обрабатывается (циркулирует) информация, содержащая сведения, отнесенные к государственной или служебной тайне, а также сами помещения, предназначенные для секретных переговоров.

Основными источниками угроз в сфере информационной безопасности являются деятельность иностранных разведывательных и специальных служб, преступных групп и формирований, противозаконная деятельность отдельных лиц, нарушение установленных регламентов сбора, обработки и передачи информации, преднамеренные действия и непреднамеренные ошибки персонала информационных систем, отказы технических средств и сбои программного обеспечения в информационных и телекомуникационных системах.

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

предотвращение перехвата с помощью технических средств информации, передаваемой по каналам связи;

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

предотвращение утечки обрабатываемой информации за счет побочных электромагнитных излучений и наводок, создаваемых функционирующими техническими средствами, а также электроакустических преобразовании;

предотвращение специальных программно-технических воздействий, вызывающих 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 организационно-технических и режимных мероприятий.

Исключение несанкционированного доступа к 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, аппаратных средств защиты, средств активного противодействия, экранированием зданий или отдельных помещений, установлением

контролируемой зоны вокруг средств информатизации И другими организационными и техническими мерами.

Предотвращение специальных программно-технических воздействий, вызывающих разрушение, уничтожение, искажение информации или сбои в работе средств информатизации, достигается применением специальных программных и аппаратных средств защиты (антивирусные процессоры, антивирусные программы), организацией системы контроля безопасного программного обеспечения.

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

Предотвращение перехвата техническими средствами речевой информации из помещений и объектов достигается применением специальных средств защиты, проектными решениями, обеспечивающими звукоизоляцию помещений, выявлением специальных устройств подслушивания и другими организационными и режимными мероприятиями.

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

лицензирование деятельности предприятий в области защиты информации;

аттестация объектов информатизации по выполнению требований обеспечения защиты информации при проведении работ со сведениями соответствующей степени секретности;

сертификация средств защиты информации и контроля за ее эффективностью, систем и средств информатизации и связи в части защищенности информации от утечки по техническим каналам;

введение территориальных, частотных, энергетических, пространственных и временных ограничений в режимах использования технических средств, подлежащих защите;

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

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

применение специальных методов, технических мер и средств защиты, исключающих перехват информации, передаваемой по каналам связи.

Конкретные методы, приемы и меры защиты информации разрабатываются в зависимости от степени возможного ущерба в случаях ее 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 и престижу Российской Федерации;

незапатентованные технологии, ноу-хау, промышленные образцы, модели и экспериментальное оборудование, для которых еще не определен статус конфиденциальности и Которые поэтому не подпадают под действующее законодательство и могут быть проданы или переданы за рубеж;

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

Специфика угроз перечисленным объектам информационной безопасности состоит в их многообразии, сложности идентификации, поскольку, как правило, они носят уникальный или индивидуальный характер» При классификации угроз в этой области необходимо уделять особое внимание изучению возможности промышленного шпионажа специальных служб и криминальных структур.

Вследствие этой специфики объекты информационной безопасности в области науки, техники и технологии трудно защитимы. Должна быть 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 использования научной, технической и технологической продукции с целью предотвращения незаконного присвоения или Использования научного и интеллектуального потенциала.

Реальный Путь противодействия угрозам со стороны государства 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, лежат в сфере социальной и экономической политики государства.

В сфере духовной жизни и информационной безопасности личности

Объектами информационной безопасности в духовной сфере являются мировоззрение людей, их жизненные ценности и идеалы, социальные и личностные ориентации, их культурные и эстетические позиции. Оценка последствий тех или иных информационных воздействий в этой сфере весьма затруднительна и должна производиться с учетом конкретно складывающейся обстановки.

Сфера духовной жизни весьма чувствительна к информационно-пропагандистскому воздействию, идеологическому давлению, культурной экспансии, которые осуществляются, главным образом, через средства массовой информации и могут рассматриваться как информационные угрозы духовному здоровью населения страны. Средства массовой информации играют определяющую роль в формировании духовной жизни. В этом состоит их особая ответственность перед обществом.

Сами информационные воздействия осуществляются в гибких, постоянно изменяющихся формах, что обусловливает сложность определения их влияния на различные составляющие духовной сферы. Это особенно характерно для современного периода развития России, когда по существу не сформулированы национальные приоритеты и идеология перестраивающихся общества и государства.

Предотвращение и нейтрализация угроз информационной безопасности в сфере духовной жизни требуют, прежде всего, открытого провозглашения государственной, официальной идеологии, приемлемой для большинства населения и учитывающей культурные и исторические традиции многонациональной страны. Лишь на основе такой идеологии могут быть выработаны четкие критерии оценки угроз информационной безопасности, основные приоритеты и государственная политика в этой сфере.

Главным представляется разработка и осуществление цивилизованных, демократических форм и методов воздействия на средства массовой информации в целях формирования и распространения духовных ценностей, отвечающих национальным интересам страны, воспитания гражданского и патриотического долга и защиты от враждебной или недружественной пропаганды.

Необходимо также разработать специальные правовые и организационные мероприятия, препятствующие коммерциализации культуры и обеспечивающие сохранение и развитие информационных ресурсов, составляющих большую культурно-историческую ценность.

Основным носителем духовных ценностей является личность, постоянно испытывающая информационные воздействия, направленные на формирование ее отношения к действительности, идеалов и устремлений, мотиваций и уровня

притязаний. Эти воздействия могут создавать эмоциональный дискомфорт, вызывать стрессы и нарушать физическую, социальную или духовную целостность личности.

Обеспечение информационной безопасности личности означает ее право на получение объективной информации и предполагает, что полученная человеком из разных источников информация не препятствует свободному формированию и развитию его личности. В качестве воздействия на личность может выступать:

целенаправленное информационное давление с целью изменения мировоззрения, политических взглядов и морально-психологического состояния людей;

распространение недостоверной, искаженной, неполной информации; использование неадекватного восприятия людьми достоверной информации.

Особую роль в воздействии на сознание и поведение отдельной личности играют средства массовой информации, которые в силу своей общедоступности и распространенности оказывают непосредственное влияние на мировоззренческие установки, субъективные ценности и предпочтения, регуляцию поступков и взаимодействие с другими людьми.

При организации противодействия угрозам информационной безопасности личности необходимо учитывать индивидуальные и личностные особенности людей, сформированные предыдущим опытом, мотивами и интересами, интеллектуальным уровнем, социально-демографическими характеристиками, социальным статусом, стереотипами и другими факторами.

Выбор адекватных способов воздействия (убеждения, внушения, разъяснения), адекватных средств (аудио, визуальных, электронных, печатных) зависят от полноты учета всех характеристик личности и ситуации. Одним из важнейших способов противодействия является упреждающее информационное воздействие.

Устойчивость к воздействиям извне определяется личностными качествами человека, которые во многом определяются постоянными информационными воздействиями, главным образом со стороны средств массовой информации. Они несут основную ответственность за формирование личностных и гражданских качеств, способных противостоять информационным угрозам. Особенно это важно в настоящее время, когда в обществе проявляются низкий уровень правосознания, непонимание людьми ценности информации.

Информационные угрозы, вызывающие сознательные или непреднамеренные нарушения информационной безопасности лиц, работающих в информационных системах и средствах массовой информации, должны парироваться посредством разъяснения их прав, регламентации обязанностей и

разделения ответственности, обучения и тренинга персонала, а в особо важных случаях — путем отбора специалистов по психологическим критериям.

V. ОСНОВЫ ГОСУДАРСТВЕННОЙ ПОЛИТИКИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ

5.1. Основные положения государственной политики обеспечения информационной безопасности Российской Федерации

Государственная политика обеспечения информационной безопасности в Российской Федерации (далее — Государственная политика) формирует направления деятельности органов государственной власти и управления в области обеспечения информационной безопасности, включая гарантии прав всех субъектов на информацию, закрепление обязанностей и ответственности государства и его органов за информационную безопасность страны, и базируется на соблюдении баланса интересов личности, общества и государства в информационной сфере.

Государственная политика является открытой и предусматривает информированность общества о деятельности государственных органов и общественных институтов в области информационной безопасности с учетом ограничений, предусмотренных действующим законодательством.

Государственная политика исходит из принципа безусловного правового равенства всех участников процесса информационного взаимодействия вне зависимости от их политического, социального и экономического статуса. Она основывается на обязательном обеспечении прав граждан и организаций на свободное создание, поиск, получение и распространение информации любым законным способом, В этих целях государство совершенствует существующее и разрабатывает новое законодательство и нормативно-правовую базу информационных отношений в обществе, а также осуществляет контроль за безусловным их исполнением.

Государство исходит из того, что информационные ресурсы являются объектом собственности, 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 включение России в глобальные информационные сети и системы мониторинга.

Исходя из принципа разделения ответственности между органами федеральной, региональной власти и местного самоуправления, государственная политика предусматривает согласованность организационных и технических решений,

принимаемых этими органами для обеспечения информационной безопасности в рамках единого информационного пространства России.

Государственная политика не допускает монополизма министерств, ведомств и организаций в области обеспечения информационной безопасности.

Государственная политика обеспечения информационной безопасности исходит из следующих основных положений:

ограничение доступа к информации есть исключение из общего принципа открытости информации и осуществляется только на основе законодательства;

ответственность за сохранность информации, ее засекречивание и рассекречивание персонифицируется;

доступ к какой-либо информации, а также вводимые ограничения доступа осуществляются с учетом определяемых законом прав собственности на эту информацию;

государство формирует нормативно-правовую базу, регламентирующую права, обязанности и ответственность всех субъектов, действующих в информационной сфере;

юридические и физические лица, собирающие, накапливающие и обрабатывающее персональные данные и конфиденциальную информацию, несут ответственность перед законом за их сохранность и использование;

государство законными средствами обеспечивает защиту общества от ложной, искаженной и недостоверной информации, поступающей через средства массовой информации;

государство осуществляет контроль за созданием и использованием средств защиты информации посредством их обязательной сертификации и лицензирования деятельности в области защиты информации;

государство проводит протекционистскую политику, поддерживающую деятельность отечественных производителей средств информатизации и защиты информации и осуществляет меры по защите внутреннего рынка от проникновения на него некачественных средств информатизации и информационных продуктов;

государство способствует предоставлению гражданам доступа к мировым информационным ресурсам, глобальным информационным сетям;

государство стремится к отказу от зарубежных информационных технологий для информатизации органов государственной власти и управления по мере создания конкурентоспособных отечественных информационных технологий и средств информатизации;

государство формирует Федеральную программу информационной безопасности, объединяющую усилия государственных организаций и коммерческих структур в создании единой системы информационной безопасности России;

государство прилагает усилия для противодействия информационной экспансии США и других развитых стран, поддерживает интернационализацию глобальных информационных сетей и систем.

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

Государственная политика в качестве механизма Согласования интересов субъектов информационных отношений и нахождения компромиссных решений предусматривает формирование и организацию эффективной работы различных советов, комитетов и комиссий с широким представительством специалистов, и всех заинтересованных структур.

Механизмы реализации Государственной политики должны быть гибкими и своевременно отражать изменения, происходящие в политической и экономической жизни страны.

5.2. Основные положения государственной политики обеспечения информационной безопасности субъектов Российской Федерации

Конституционные основы федеративного государственного устройства страны нуждаются в развитии и распространении на все сферы жизнедеятельности личности, общества и государства, включая сферу обеспечения информационной безопасности.

Информационная безопасность должна быть предметом ответственности органов государственной власти и управления всех уровней с учетом закрепленного в Конституции Российской Федерации разграничения предметов ведения и полномочии между ними.

Разработка региональных вопросов обеспечения информационной безопасности имеет ряд особенностей, объективно связанных с федеративным устройством страны.

Информационная собственность субъектов Российской Федерации является разновидностью государственной собственности субъектов Российской Федерации.

Она включает в себя:

информационную собственность органов власти и управления субъектов Российской Федерации;

информационную собственность предприятий и учреждений, созданных или приобретенных за счет средств субъектов Российской Федерации;

культурные ценности народов, населяющих территорию субъектов Российской Федерации.

Обязанностью органов власти и управления субъектов Российской Федерации является защита права информационной собственности, находящейся на территории субъектов1 Российской Федерации объектов федеральной информационной собственности, информационной собственности органов местного, самоуправления, других юридических и физических лиц.

Субъекты Российской Федерации обладают всей полнотой информационных прав, действующих в Российской Федерации. Эти права от имени субъектов Российской Федерации осуществляют их органы государственной власти и управления.

Субъектам Российской Федерации гарантируется:

равное право доступа на российский рынок информации и средств обеспечения информационной безопасности, находящихся в любой форме собственности;

право использования для решения региональных государственных задач федеральных информационных банков данных с соблюдением установленных правил обеспечения информационной безопасности;

право проведения самостоятельной внутренней и внешнеэкономической деятельности в сфере информационной безопасности в рамках, определенных федеральными законами;

право осуществлять защиту своих информационных прав и права информационной собственности как самостоятельно, так и путем обращения в федеральные и международные правозащитные органы.

Более подробная проработка основных направлений региональной политики обеспечения информационной безопасности должна быть осуществлена субъектами Российской федерации с учетом особенностей их территорий, состояния и перспектив развития хозяйственной сферы.

5.3. Правовое обеспечение информационной безопасности Российской Федерации

Правовое обеспечение рассматривается как приоритетное направление формирования механизмов реализации политики обеспечения информационной безопасности в Российской Федерации.

Правовое обеспечение включает в себя:

нормотворческую деятельность по созданию законодательства, регулирующего отношения в обществе, связанные с обеспечением информационной безопасности;

исполнительную и правоприменительную деятельность по исполнению законодательства в области информации, информатизации и защиты информации органами государственной власти и управления, организациями (юридическими лицами), гражданами.

Нормотворческая деятельность в области обеспечения информационной безопасности предусматривает:

оценку состояния действующего законодательства и разработку программы его совершенствования;

создание организационно-правовых механизмов обеспечения информационной безопасности;

формирование правового статуса всех субъектов в системе информационной безопасности, пользователей информационных и телекоммуникационных систем и определение их ответственности за обеспечение информационной безопасности;

разработку организационно-правового механизма сбора и анализа статистических данных о воздействии угроз информационной безопасности и их последствиях с учетом всех видов (категорий) информации;

разработку законодательных и других нормативных актов, регулирующих порядок ликвидации последствий воздействий угроз, восстановления нарушенного права и ресурсов, реализации компенсационных мер.

Исполнительная и правоприменительная деятельность предусматривает разработку процедур применения законодательства и нормативных актов к субъектам, совершившим преступления и проступки при работе с закрытой информацией и* нарушившим регламент информационных взаимодействий, а также правонарушения с использованием незащищенных средств информатизации, разработку составов правонарушений с учетом специфики уголовной, гражданской, административной, дисциплинарной ответственности.

Вся деятельность по правовому обеспечению информационной безопасности должна строиться на основе трех фундаментальных положений права — соблюдение законности, обеспечение баланса интересов отдельных субъектов и государства, неотвратимость наказания.

Соблюдение законности предполагает Наличие законов и иных нормативных установлений, их применение и исполнение субъектами права в области информационной безопасности.

Обеспечение баланса интересов граждан, других субъектов информационных отношений и государства предусматривает приоритет государственных интересов как общих интересов всех субъектов. Ориентация на свободы, права и интересы граждан не принижает роль государства в обеспечении национальной безопасности в целом и в области информационной безопасности в частности.

Неотвратимость наказания предусматривает соответствующую степень ответственности в области обеспечения информационной безопасности, которая реализуется с учетом повышенной социальной опасности угроз информационной среде общества.

Реализация механизмов правового обеспечения информационной безопасности должна опираться на информатизацию правовой сферы в целом.

5.4. Первоочередные мероприятия по реализации государственной политики информационной безопасности Российской Федерации

Первоочередные мероприятия по реализации государственной политики информационной безопасности Российской Федерации должны включать:

разработку форм, методов и средств реализации государственной политики, подготовку решений органов исполнительной власти и документов, закрепляющих ее основные положения;

создание нормативно-правовой базы реализации государственной политики в области информационной безопасности, в том числе определение последовательности и порядка разработки законодательных и нормативно-правовых актов, а также механизмов практической реализации принятого законодательства;

анализ технико-экономических параметров отечественных и зарубежных программно-технических средств обеспечения информационной безопасности и выбор перспективных направлений развития отечественной техники;

формирование Государственной научно-технической программы совершенствования и развития методов и средств обеспечения информационной безопасности, предусматривающей их использование в национальных информационных и телекоммуникационных сетях и системах с учетом перспективы вхождения России в глобальные информационные сети и системы;

создание системы сертификации на соответствие требованиям информационной безопасности отечественных и закупаемых импортных средств

информатизации, используемых в государственных органах власти и управления;

совершенствование организационной структуры системы информационной безопасности Российской. Федерации, предусматривающее создание единого центра координации и регулирования деятельности всех органов, входящих в систему;

разработка системы экономических и статистических показателей, характеризующих эффективность функционирования системы обеспечения информационной безопасности;

определение реальных потребностей системы информационной безопасности в специалистах, организация системы отбора, подготовки и переподготовки кадров.

VI. ОРГАНИЗАЦИОННАЯ СТРУКТУРА И ПРИНЦИПЫ ПОСТРОЕНИЯ СИСТЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ

6.1. Организационная структура системы информационной ■ безопасности Российской Федерации

Анализ состояния информационной безопасности в стране диктует необходимость реформирования существующей организации обеспечения информационной безопасности с целью создания целостной, системы обеспечения информационной безопасности Российской Федерации (далее — Система).

Система является составной частью общей системы национальной безопасности страны, представляет собой совокупность органов государственной власти и управления и предприятий, согласованно осуществляющих, деятельность по обеспечению' информационной безопасности на основе единых правовых норм.

Организационную структуру Системы составляют:

органы государственной власти и управления Российской Федерации и субъектов Российской Федерации, решающие задачи обеспечения информационной безопасности в пределах своей компетенции;

государственные и межведомственные комиссии и советы, специализирующиеся на проблемах информационной безопасности;

структурные и межотраслевые подразделения по защите информации органов государственной власти и управления, а также структурные подразделения предприятий, проводящие работы с использованием сведений, отнесенных к государственной тайне, или специализирующиеся на проведении работ в области защиты информации;

научно-исследовательские, проектные и конструкторские организации, выполняющие работы по обеспечению информационной безопасности;

учебные заведения, осуществляющие подготовку и переподготовку кадров для работы в системе обеспечения информационной безопасности.

Особое место в системе информационной безопасности занимают государственные и общественные организации, осуществляющие законный контроль за деятельностью государственных и негосударственных средств массовой информации.

6.2. Основные функции системы информационной безопасности Российской Федерации

Система информационной безопасности осуществляет свою деятельность на основе государственной политики обеспечения национальной безопасности Российской Федерации.

Основными функциями системы обеспечения информационной безопасности Российской Федерации являются:

разработка и реализация стратегии обеспечения информационной безопасности;

реализация прав граждан и организаций на получение, распространение и использование информации;

оценка состояния информационной безопасности в стране, выявление источников внутренних и внешних угроз информационной безопасности, определение приоритетных направлений предотвращения, парирования и нейтрализации этих угроз;

координация и контроль деятельности субъектов системы информационной безопасности;

организация разработки федеральных и ведомственных программ обеспечения информационной безопасности и координация работ по их реализации;

проведение единой технической политики в области обеспечения информационной безопасности;

организация фундаментальных, поисковых и прикладных научных исследований в области информационной безопасности;

обеспечение контроля за созданием и использованием средств защиты информации посредством обязательного лицензирования деятельности в области защиты информации и сертификации средств защиты информации;

осуществление международного сотрудничества в сфере информационной безопасности, представление интересов Российской Федерации в соответствующих международных организациях.

Система должна обеспечивать гибкое управление процессами информационной безопасности на государственном, региональном, отраслевом, производственном и пользовательском уровнях.

Масштабность, сложность и разнообразие перечисленных функций требуют создания иерархической организационной структуры, обеспечивающей координацию деятельности всех составляющих системы информационной безопасности.

Построение Системы осуществляется на основе разграничения предметов ведения и полномочий федеральных и региональных органов государственной власти, с учетом согласованности деятельности территориальных органов федеральной исполнительной власти и органов власти субъектов Российской Федерации.

VII. МЕЖДУНАРОДНОЕ СОТРУДНИЧЕСТВО ПО ВОПРОСАМ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

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

Сотрудничество должно способствовать повышению информационной безопасности всех членов мирового сообщества, включая Российскую Федерацию.

Основными направлениями сотрудничества, отвечающими интересам Российской Федерации, являются:

предотвращение несанкционированного доступа к конфиденциальной информации в международных банковских сетях и в каналах информационного обеспечения мировой торговли, к конфиденциальной 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 расщепляющимися материалами;

обеспечение информационной безопасности трансграничного информационного обмена и его информационного регламента, а также сохранности и неискаженности информации при ее передаче по национальным телекоммуникационным каналам и каналам связи;

координация деятельности государств — участников международного сотрудничества по предотвращению компьютерных преступлений.

Особое внимание в ходе сотрудничества должно быть уделено проблемам взаимодействия со странами СНГ с учетом перспектив создания единого информационного пространства на территории бывшего СССР, в пределах которого используются практически единые телекоммуникационные системы и линии связи.

Для реализации указанных направлений сотрудничества необходимо:

активное участие России во всех международных организациях, действующих в области информационной безопасности;

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

расширение участия российских специалистов в международных конференциях, семинарах, выставках.

Для разработки методологических и научно-технических проблем обеспечения международной информационной безопасности целесообразно создание под эгидой ООН Международного научно-исследовательского института.

ОСНОВНЫЕ ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Документированная информация - зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать.

Защита информации - организационные, правовые, технические и технологические меры по предотвращению угроз информационной безопасности и устранению их последствий.

Информационная безопасность - состояние защищенности информационной среды общества, обеспечивающее ее формирование и развитие в интересах граждан, организаций и государства.

Информационная среда - совокупность информационных ресурсов, общества система формирования, распространения и использования информации, информационной инфраструктуры.

Информационная инфраструктура - совокупность центров обработки и анализа информации, каналов информационного обмена и телекоммуникации, линий связи, систем и средств защиты информации.

Информация - сведения о лицах, предметах, событиях, явлениях и процессах, независимо от формы их представления.

Информационные ресурсы - данные и документированная информация о жизнедеятельности общества, организованная, в базы и банки данных, а также другие формы организации информации.

Угрозы информационной безопасности - фактор или совокупность факторов, создающих опасность функционированию и развитию информационной среды общества.

Информация с ограниченным доступом - информация, для которой установлен специальный режим сбора, хранения, обработки, распространения и использования.

Несанкционированный доступ к информации - доступ к информации, нарушающий установленные правила получения информации.