На правах рукописи

ЛЕВИН Александр Алексеевич

ПРИОРИТЕТНЫЕ НАПРАВЛЕНИЯ ДЕЯТЕЛЬНОСТИ ГОСУДАРСТВА ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ

(политологический анализ)

Специальность 20.01.02 - Стратегия. Военные аспекты безопасности государства, военная политология

АВТОРЕФЕРАТ

диссертации на соискание ученой степени кандидата политических наук

Москва - 2004

Работа выполнена на кафедре национальной безопасности Российской академии государственной службы при Президенте **РФ**

Научный руководитель - доктор политических наук, доцент
ВОЗЖЕНИКОВ Анатолий Васильевич

Официальные оппоненты: доктор политических наук, профессор
ЯВЧУНОВСКАЯ Регина Анатольевна

кандидат политических наук
СИНЕОК Николай Васильевич

Ведущая организация: Институт **научной информации по общественным наукам РАН**

Защита состоится "___"_____2004 г. р_____часов на заседании диссертационного совета ДСПР 502.001.02 при Российской академии государственной службы при Президенте Российской Федерации по адресу: 119606, Москва, пр. Вернадского, 84, 1-й учебный корпус, ауд._____.

С диссертацией можно ознакомиться в библиотеке Российской академии государственной службы при Президенте Российской Федерации.

Автореферат разослан "____"_____2004 г.

Ученый секретарь
диссертационного совета,
кандидат юридических наук, доцент Н.В. Кривельская

ОБЩАЯХАРАКТЕРИСТИКАРАБОТЫ

Актуальность исследования. В XXI веке система обеспечения информационной безопасности Российской Федерации, как и многих других современных государств, столкнулась с рядом факторов, негативно воздействующих на возможности государства эффективно обеспечивать защиту ее национальных интересов в информационной сфере. Среди внешних факторов наиболее опасным представляется процесс глобализации[1], сопровождающийся навязыванием странам и народам западных ценностей и подрывом их традиционных ценностей с помощью новых информационно-телекоммуникационных систем и технологий (ИТКСТ).

Кроме того, высокая результативность использования ИТКСТ, широкий спектр их применения и скрытый характер воздействия явились причинами, по которым многие страны ведут разработки в области теории и практики их применения в качестве информационного оружия и, как следствие, разработки теории ведения информационных войн[2].

Внутренним фактором, снижающим уровень информационной безопасности России, стал процесс либерально-демократических реформ российского общества, в котором не в полной мере учитываются интересы и потребности основных объектов безопасности.

В этих условиях сложившаяся ранее система обеспечения информационной безопасности РФ явно не соответствует новым

[1] См., например: Геллени Р.Д., Маккой М. Глобализация и независимая политика в области налогообложения // Реф. бюллетень. Государственная служба за рубежом. Глобализация. Экономические аспекты. - 2002. - № 5. - С. 109. Под «глобализацией» авторы понимают «растущую интеграцию международных рынков, происходящую в силу быстрого роста мировых потоков товаров, услуг, капиталов, информации и (иногда) людей, ставшего возможным благодаря росту торговой взаимозависимости между странами».

[2] См.: Поздняков А. Информационная война за влияние в мире и политическую власть // Власть. - 1996. - №10.-С. 49-54.

принципам обеспечения информационной безопасности и не может надежно противодействовать информационным угрозам. Поэтому в настоящий период развития России остро встал вопрос определения приоритетов, в области государственной политики обеспечения информационной безопасности и сосредоточения усилий на наиболее важных участках потенциальных и реальных угроз.

Кроме того, в условиях расширяющейся информатизации российского общества, когда информация становится товаром и ресурсом развития, наращивания политической, экономической, военной и духовной мощи государства, когда информационная сфера безопасности все больше и больше выступает системообразующим фактором всей многоуровневой системы обеспечения безопасности личности, общества и государства, определение приоритетных направлений деятельности государственных органов страны по обеспечению информационной безопасности становится важнейшей политической и теоретической задачей[1].

Россия остро нуждается в эффективной политике обеспечения безопасности своих национальных интересов в информационной сфере, учитывающей объективные реалии современной информационной среды и основанной на научно-методической базе[2]. Она позволит государственным органам власти отойти от рефлексивного стиля управления информационной безопасностью РФ и направить свою деятельность на предотвращение угроз в информационной сфере. Автор полагает, что анализ деятельности государственных органов власти в области обеспечения информационной безопасности РФ будет способствовать созданию необходимой базы для

[1] См.: Возжеников А.В. Защита сознания // Россия: третье тысячелетие. Вестник актуальных прогнозов. - 2001. - №3. - С. 61.

[2] См., например: Концепция национальной безопасности РФ (Указ Президента РФ от 10. 01. 2000 г., № 24) // Российская газета. - 2000. - 18 янв.; Шийко А.С. Компьютерная преступность как угроза информационной безопасности РФ. Дис. на соиск. уч. ст. канд. полит, наук. - М.: РАГС. - 2000.

теоретических обобщений, а результаты сопоставления реального уровня информационной безопасности России с потребностями общественного развития помогут сформировать представление о выборе приоритетов в области реализации государственной политики обеспечения информационной безопасности.

Таким образом, актуальность диссертационного исследования обусловлена:

1. Степенью значимости проблемы;

2. Наличием реальных и потенциальных угроз национальным интересам РФ в информационной сфере;

3. Потребностью государственных органов власти в оптимальном использовании ограниченных государственных ресурсов и необходимостью эффективно решать данную управленческую задачу в условиях становления информационного общества в России и его вхождение в мировое информационное пространство.

Степень научной разработанности темы. Научное осмысление информационной безопасности как деятельности государственных институтов власти по защите национальных интересов РФ от угроз **в** информационной сфере значительно активизировалось в последнее десятилетие. Вместе с тем, несмотря на значительное количество работ, посвященных изучению информационной безопасности, очень мало в этой области комплексных исследований, связывающих теорию обеспечения безопасности и государственную политику.

Исследования и разработки по изучаемой теме условно можно разделить на семь групп.

К первой группе относятся научные работы Возженикова А.В., Нуждина Ю.Ф., Стрельцова А.А., Цыгичко В.Н, Черешкина Д.С.,

Смолян Г.Л., Панарина И.Н., Позднякова А.И.; Почепцова Г.Г., Прохожева А.А., Расторгуева СП., ШийкоА.С. и др., изучающие политологические аспекты обеспечения национальной и информационной безопасности **РФ**[1]**.**

Ко второй группе относятся научные работы Грачева Г.В., Ермакова Ю.А., Лепского В.Е., Мельник И.К., Панарина И.Н., Панарина А.С., связанные с изучением проблем защиты личности от вредного информационного воздействия.

К третьей группе относятся научные работы Антопольского А.А. (2002 г.), Балыбердина А.Л. (1999 г.), БачилоИ.Л. (2001г.), КиринаВ.И. (2000 г.), Колобова О.А. и Ясенева В.Н. (2001 г.), Копылова В.А. (2002 г.), Лопатина В.Н. (2002 г.), Огородова Д.В. (2002 г), Просвирина Ю.Г.(2001 г) Фатьянова А.А. (2001г.), анализирующие правовые аспекты защиты интересов личности в информационной сфере. В большей степени усилия данных авторов сосредотачивались на правовом обеспечении защиты информации, развитии законодательной базы и совершенствовании правоприменительной практики в области информатизации.

К четвертой группе относятся научные исследования Боер В.М. (1998 г.), Клебанова Л.Р. (2002 г.), Костенко М.Ю. (2002 г.), Кузьмина СВ.

[1] См.: Возжеников А.В. Национальная безопасность: теория, политика, стратегия. - М.: НПО «Модуль», 2000; .Национальная безопасность в контексте современного политического процесса России: Теория и политика обеспечения: Дис. на соиск. уч. ст. д-ра полит, наук. - М., 2002; Стрельцов А.А. Обеспечение информационной безопасности России. Теоретические и методологические основы / Под. ред. В.А. Садовничего и В.П. Шерспока. - М.: МЦНМО, 2002; ЦыгичкоВ.Н., Смолян ГЛ., ЧерешкинД.С. Информационное оружие как геополитический фактор и инструмент силовой политики. М: ИСА РАН. 1997; Панарин И.Н. Информационно-психологическое обеспечение национальной безопасности России. Дис. на соиск. уч. ст. д-ра полит, наук. - М., 1998; Почепцов Г.Г. Информационные войны. - М.: Реф-бук, Ваклер, 2000; Прохожее А.А. Информационная безопасность - важнейшая составляющая национальной безопасности современной России. - М, 1996; Национальная безопасность: основы теории, сущность, проблемы. - М.: РАГС, 1997.; Расторгуев СП. Философия информационной войны. - М.: Вузовская книга, 2001; Грачев Г.В. Информационно-психологическая безопасность личности: состояние и возможности психологической защиты. - М.: Институт психологии РАН, 1999; Ермаков Ю.А. Манипуляция личностью: смысл, приемы, последствия. - Екатеринбург, 1995. Основы национальной безопасности России / Под ред. В_Л. Манилова. - М.: Друза, 1998;

(2000 г.), Кузнецова П.У. (2001 г.), Кленова С.Н. (2002 г.), Ревинского О.В. (2000 г.), РевякоТ.И. (1997 г.), Толубековой Б.Х. (1998 г.), Ушакова СИ. (2001 г.), Шийко А.С. (2000 г.), монографии Иванского В.П. (1999 г.), Тер-АкоповаА.А. (1998 г.) связанные с возможностями субъектов безопасности противодействовать информационным преступлениям.

К пятой группе относятся работы Герасименко В.А., Зегжды М.П., ГриняеваС.Н. (1999 г.), Лопатина В.Н. (1999 г.), Сычева М.П., Ухлинова Л.М., Цыганкова В.Д. (1999 г.), ЦыгичкоВ.Н. (2000 г.), Шурухнова Н.Г. (1999 г.), Никитова В.А., Орлова Е.И., Старовойтова А.В., Савина Г.И. (2000 г.), связанные с изучением технических аспектов защиты информации в информационных системах и сетях.

К шестой **группе** относятся научные работы Андрианова Д.А. (2002 г.), Брусницына Н.А. (2001г.), Кузнецова В.Н. (2000 г.), Митрохина Е.Ю. (1999 г.), Павленко С.З. (1998 г.), Панарина И.Н. (2001 г.), Рабовского СВ. (2001г.), Расторгуева СП. (2000 г.), Федорова А.В. (2001г.), монография Возженикова А.В. (2000 г.), Василенко Л.А. (1999 г.), Забелина И.В. (2001 г.), затрагивающие разные аспекты защиты информации.

К седьмой группе можно отнести научные работы зарубежных ученых АхвельдтаХ. (2001 г.), БейкераУ.Е. (2000 г.), БекаУ.С (2000 г.), Белла Д.С. (1999 г.), Веллерсхофа Д. (1999 г.), Грея Д. (2001 г.), ДенхардтаР. (2000 г.), КуродыХ. (2000 г.), КалдораМ. (2001г.), ЛорантаК. (2002 г.), ПакеК.Х. (2001 г.), ПеттисаМ. (2001 г.), ТоффлераО. (2000 г.), изучающие национальные интересы, ценности общества в условиях становления единого информационного пространства[1].

[1] **См., например: Белл Д. Грядущее постиндустриальное общество. Опыт социального прогнозирования / Пер. с англ. - М, 1999; Бек У. Общество риска. На пути к другому модерну / Пер. с нем. В. Седельника и Н. Федоровой. - М.: Прогресс-Традиция, 2000.**

Определяя приоритеты государственной политики в области обеспечения информационной безопасности российского общества в контексте современного развития, автор использовал результаты отечественных и зарубежных ученых, а также результаты авторского исследования. Исследование показало, что такого комплексного междисциплинарного исследования в отечественной политологической науке не проводилось.

Объект исследования - государственная система обеспечения информационной безопасности РФ.

Предмет исследования - государственная политика обеспечения информационной безопасности РФ в современных условиях.

Рабочая гипотеза: в современных условиях формирования рыночных отношений и становления информационного общества отсутствие научно обоснованных приоритетов в государственной политике обеспечения информационной безопасности РФ не позволяет государственным институтам власти создать и постоянно поддерживать уровень защищенности жизненно важных интересов всех объектов безопасности, адекватный угрозам в информационной сфере.

Научная задача, решаемая в соответствии с рабочей гипотезой, состоит в теоретико-прикладном исследовании современной деятельности государственных институтов власти в области обеспечения информационной безопасности РФ с целью повышения эффективности проводимой политики.

Цель исследования — определение приоритетов в государственной политике обеспечения информационной безопасности РФ и разработка на этой основе практических рекомендаций по рационализации деятельности государственных институтов власти в целях повышения уровня

защищенности национальных интересов РФ в информационной сфере.

Задачи исследования, главными из которых являются:

- обоснование выбора концепции исследования политики информационной безопасности;

- оценка эффективности деятельности государственных органов власти в области обеспечения информационной безопасности РФ;

- определения приоритетных направлений государственной политики по обеспечению информационной безопасности **РФ.**

Границы исследования определяются современным этапом развития общественных отношений (1992-2004 г.), соответствующие становлению в РФ информационного общества.

Научная новизна работы и полученных результатов состоит:

- в проведении политологического анализа деятельности государственных органов власти в области обеспечения информационной безопасности в новых условиях развития информационной среды и реализации Доктрины информационной безопасности РФ;

- в проведении социологического исследования на тему: «Уровень информационной безопасности предприятий ОПК в представлениях руководителей узлов связи, входящих в государственную корпоративную информационную систему РФ» (N=78);

- в оценке уровня информационной безопасности РФ на основе метода определения уровня защищенности жизненно важных интересов от угроз;

- в обосновании объективной необходимости и жизненной потребности определения приоритетов в деятельности государственных органов власти в области обеспечения информационной безопасности РФ.

Теоретическая основа исследования представлена общей теорией

национальной безопасности, теорией интересов, теоретическими разработками отечественных и зарубежных ученых в области информатизации, информационной безопасности. Особый акцент автор делает на теории информационного общества.

Методологическая основа исследования представляет собой синтез подходов, выбор которых обусловлен необходимостью обеспечить достижение поставленной цели. В диссертации использовались: системный подход, метод сравнительного анализа, синергетический, функциональный подходы.

Решая задачи диссертационного исследования, соискатель руководствовался принципом диалектической взаимосвязи и взаимозависимости социальных явлений, сравнительным и ценностным подходами. Системный подход используется в работе как универсальный метод, применяемый в изучении проблем национальной безопасности. Исследование частных вопросов производится автором посредством: метода включенного наблюдения, метода экспертных опросов, метода структурно-функционального анализа, факторного и логического методов.

Эмпирическую базу исследования составляют:

- результаты традиционного анализа государственных документов в области обеспечения информационной безопасности;
- статистические данные государственных и негосударственных организаций;
- результаты авторского социологического опроса экспертов ОПК РФ- в области информационной безопасности (N=78 респондентов);
- результаты включенного наблюдения (в ходе профессиональной деятельности автора с 1979-2001 гг.);

- вторичный анализ результатов социологических исследований компании Ernst & Young в области информационной безопасности организаций России, использующие корпоративные информационные сети.

Теоретическая **значимость исследования** заключается в расширении сферы научного знания о содержании информационной безопасности в контексте современного политического процесса; в обосновании использования системного подхода к изучению проблем информационной безопасности как сложной многоуровневой развивающейся социальной системы, состоящей из подсистем, взаимосвязанных в контексте политической жизни; в обосновании необходимости определения приоритетов в государственной политике обеспечения информационной безопасности.

Основные положения, выносимые на защиту:

1. Обоснование роли государственной политики в обеспечении информационной безопасности РФ.
2. Классификация угроз информационной безопасности РФ на основе внешних и внутренних источников опасности и их общей направленности на объект.
3. Результаты политологического анализа деятельности государственных органов власти в области обеспечения информационной безопасности РФ.
4. Приоритетные направления политики государства в области обеспечения информационной безопасности.

Практическая значимость работы состоит в определении приоритетов в государственной политике обеспечения информационной безопасности РФ, что, по мнению соискателя, будет способствовать:

достижению стратегических целей, обозначенных в Доктрине информационной безопасности РФ; эффективной деятельности федеральных органов государственной власти и органов государственной власти субъектов РФ в этой области; повышению уровня защищенности государственных и корпоративных информационных сетей в России.

Вместе с тем сама диссертационная работа может быть использована в качестве учебного материала для вузовской программы (курс «Информационная безопасность»). Это придаст ей практическую направленность, позволит сконцентрировать внимание обучаемых на реальных угрозах информационной безопасности, факторах, порождающих эти угрозы, на принятии необходимых мер по защите национальных интересов.

Апробация результатов исследования. Многие из положений, выносимых на защиту, апробированы автором в своих выступлениях на международных и отечественных конференциях (РАГС, 2001 г. и 2002 г.; ИНИОН РАН, в 2002 г.)[1]; в публикациях в российских научных изданиях. Материалы социологического исследования, проведенного автором, использованы в практической. работе общественной организации Фонд «Отечество», коммерческой фирмы «ЭДАС ПАК».

Структура диссертации. Работа состоит из введения, двух глав, заключения, библиографического раздела и приложений.

ОСНОВНОЕ СОДЕРЖАНИЕ ДИССЕРТАЦИИ

Во **введении** обосновывается актуальности темы, определяется

[1] См.: Материалы I научно-практической конференции «Проблемы внутренней безопасности России в XXI веке». - М.: РАГС, фонд «Отечество», 2001; Материалы II научно-практической конференции «Проблемы внутренней безопасности России в XXI веке». - М.: РАГС, фонд «Отечество», 2003, Материалы II Международной научной конференции «Россия: тенденции и перспективы развития». 13-14 дек. 2001. - М.: ИНИОН РАН, 2002; Материалы III Международной научной конференции «Россия: тенденции и перспективы развития». 16-17 дек. 2002. - М.: ИНИОН РАН, 2003.

степень ее разработанности в научной литературе, формулируются основная цель и задачи исследования, его теоретическая и эмпирическая база, отмечается научная новизна и практическая значимость работы, констатируется рабочая гипотеза авторского исследования.

В первой главе - «Теоретико-методологические основы исследования политики информационной безопасности как элемента системы обеспечения информационной безопасности» - рассматриваются методологические основы исследования информационной безопасности, понятия «угроза безопасности», «информационная безопасность» и «политика, информационной безопасности», обосновывается выбор методологии исследования.

Автор, рассмотрев научную категорию «информационная безопасность», данную в нормативно-правовых документах РФ[1], Доктрине информационной безопасности РФ, считает ее неполной, так как в первом случае объектом защиты является вся информационная среда, во втором - национальные интересы. И в научной литературе отсутствует единая точка зрения на содержание понятия «информационная безопасность», которую одни ученые рассматривают как состояние, другие как процесс, деятельность, систему гарантий и т.д.

Таким образом, категорию «информационная безопасность» автор рассматривает как **состояние** защищенности жизненно важных интересов личности, общества и государства в информационной сфере от внутренних и внешних угроз и **процесс** противодействия этим угрозам обеспечивающий устойчивое развитие в настоящий и в будущий момент времени.

[1] **ФЗ «Об участии в международном информационном обмене» СЗ РФ. - М., 1996. -№ 28. - Ст. 3347.**

Опираясь на общую теорию национальной безопасности[1], под обеспечением информационной безопасности автор понимает целенаправленную деятельность государственных институтов власти, общественных и коммерческих организаций, а также граждан по выявлению, предупреждению угроз безопасности личности, общества и государства в информационной сфере и противодействию им в целях защиты жизненно важных интересов.

На практике эта деятельность определяется государственной политикой обеспечения информационной безопасности Российской Федерации и отражается в деятельности органов государственной власти и управления. Основные направления этой деятельности определяются жизненно важными интересами объектов безопасности в информационной сфере, характером и выраженностью реальных и потенциальных угроз по отношению к этим интересам, необходимостью выработки эффективных методов в достижении поставленной цели. В свою очередь, приоритетные направления определяются политическим руководством страны при корректировке стратегии и решения главных задач в области обеспечения информационной безопасности РФ.

Выше изложенное предопределило использование общей теории национальной безопасности и выбор методологии исследования информационной безопасности как область деятельности субъектов безопасности, имеющие свои жизненно важные интересы, предопределяющие их цели и задачи, которые в тоже время взаимосвязаны между собой посредством политической жизни.

Однако, автор считает, что существующая методология

[1] См.: Общая теория национальной безопасности: Учебник / Под общ. ред. д. э. н., проф. А.А. Прохожева. - М.: Изд-во РАГС, 2002. - С. 149.

исследования различных предметных сторон информационной безопасности в теоретическом плане разработана недостаточно и требует своего дальнейшего развития и совершенствования в контексте изменяющихся условий современной действительности. В то же время применение общей теории национальной безопасности и методологии комплексного исследования национальной безопасности позволили автору исследовать политику обеспечения информационной безопасности РФ.

Анализ внешних угроз информационной безопасности РФ показал, что в условиях нарастающей конкуренции многие государства все шире используют информационную сферу для достижения собственных национальных целей. В политической сфере возрастает значимость применения информационно-психологического воздействия на интересы, цели, ценности других государств. В экономической сфере растет уязвимость экономических структур в связи с незаконным использованием информации конкурентами. В военной сфере исход вооруженных конфликтов между противоборствующими сторонами все более определяется имеющимся объемом информационно-технического и информационно-психологического потенциала и его использованием.

На основе проведенной оценки внешних угроз информационной безопасности РФ автор делает вывод, что они имеют объективный характер, обусловлены современным политическим процессом и тесно связаны с изменениями в информационной сфере на основе развития и применения новейших информационных систем и технологий. Выявленная закономерность выражается в расширении масштабов угроз информационной безопасности РФ со стороны иностранных государственных организаций, различных организаций и граждан этих стран, что нашло свое отражение в основных направлениях

государственной политики обеспечения информационной безопасности РФ[1].

Однако, для выделения приоритетных задач в области политики обеспечения необходимы анализ состояния жизненно важных интересов в информационной сфере и на его основе определение реальных угроз. Автор предпринял классификацию-угроз информационной безопасности РФ, исходя из наличия внутренних и внешних источников (табл. 1).

Таблица 1

Классификация угроз информационной безопасности РФ по характеру направленности на объект

Реальные	Потенциальные
Противоправный доступ к конфиденциальной информации	Противоправный сбор и использование информации
Манипулятивное воздействие на сознание личности, социальной группы	Деструктивное воздействие на духовные ценности общества
Деструктивное воздействие на психику личности, социальной группы	Создание средств опасного воздействия на объекты безопасности

Анализ угроз информационной безопасности РФ показал, что количество угроз и формы их проявления увеличиваются быстрее, чем появляются доступные средства защиты от них. Так, в экономической, политической, военной и духовной сферах имеют место противоправный доступ к конфиденциальной информации, манипуляция сознанием личности, социальной группы и деструктивное воздействие на их психику.

[1] См.: Доктрина информационной безопасности РФ. - М.: 2000 г.

Автор приходит к выводу, что уровень информационной безопасности РФ снижают следующие факторы: несовершенство правовых механизмов в информационной сфере; просчеты в социально-экономической политике; отставание отечественной технологической базы; нерегламентированная закупка информационной техники за рубежом; низкий профессионализм управленческих кадров и др. Анализ этих факторов и угроз безопасности стал основой в определении реальных интересов субъектов информационной безопасности и деятельности государственных институтов власти по достижению поставленных целей в области обеспечения информационной безопасности **РФ.**

Во второй главе - «Определение приоритетов государственной политики в области обеспечения информационной безопасности» - анализируется деятельность государственных институтов власти по выявлению, предупреждению и противодействию угрозам безопасности, приведенным в табл. 1.; обосновывается выбор приоритетных направлений в государственной политике обеспечения информационной безопасности РФ и рекомендуются меры, повышающие ее эффективность.

Для решения поставленной задачи автор проводит оценку уровня информационной безопасности личности, общества и государства. Результаты оценки, подтверждая гипотезу, позволяют установить значительные отклонения результатов деятельности государственных институтов власти в области обеспечения информационной безопасности РФ от главной цели — создание и поддержание необходимого уровня защищенности жизненно важных интересов основных объектов безопасности от угроз в информационной сфере, гарантированных Конституцией РФ, принятыми законами и

политическими документами.

Имеющие место случаи незащищенности личной, государственной и корпоративной информации обусловлены ущемлением интересов личности и корпоративных групп в информационной и социально-экономической сферах. Вследствии этого в обществе отмечается рост преступности и наносимый ею ущерб. По статистике МВД России в 2000 г. зарегистрировано 1375 компьютерных преступлений, а по данным общественной организации CERT в тот же период - 15167. Рост преступлений в сфере информационных технологий только по компьютерным преступлениям в 2001 г. составил более 3 тыс., в 2002 г. - свыше 5600, в 2003 г. - 10920, из которых более 90% связано с противоправным доступом к информации. В свою очередь, доходы от этих преступлений сопоставимы с доходами от продажи оружия и наркотиков[1]. Другие источники сообщают, что Российской Федерации ежегодно наносится ущерб в размере 500 млн долларов США только из-за бесконтрольного вывоза из страны научных разработок и компьютерных программ. Аналитики в свою очередь отмечают, что Россия недополучает ежегодно в бюджет страны от 17 до 30 млрд долларов из-за бесконтрольной продажи информации. Факты свидетельствуют о неэффективной деятельности системы обеспечения информационной безопасности РФ, которая не обеспечивает соответствующий уровень защищенности жизненно важных интересов основных объектов безопасности, адекватный угрозам.

Следует особо подчеркнуть, что в преступную деятельность вовлекаются прежде всего интеллектуальные слои российского общества:

[1] **См.: Авчаров И.В. Аспекты взаимодействия ведомств и организаций в вопросах борьбы с преступлениями в информационной сфере. Матер, конф. Инфофорум - 5.2003 г. 5 февр. - www.infoforum.ru**

инженеры, врачи, военнослужащие, профессиональные группы работников милиции, суда и прокуратуры, ФАПСИ, ФСБ, ФПС, СВР, МЧС, таможни, налоговой службы. Это подтверждает правильность классификации угроз, предложенную автором в I главе, а также указывает на не достаточный учет принципа баланса интересов в деятельности государственных органов власти при принятии решений.

Результаты социологических опросов свидетельствуют, о низком профессионализме кадров государственной службы, служащих различных корпораций, их способности в определении целей и задач по противодействию угрозам в информационной сфере.

Руководители государственных и негосударственных организаций, использующие корпоративные информационные сети, обеспечение информационной безопасности своих организаций рассматривают в основном с позиции решения технических задач. Авторский анализ результатов социологических исследований негосударственных организаций указывает на то, что лишь 16% из числа опрошенных респондентов считают личное участие руководителя организации в политике обеспечения безопасности необходимым, 30% - ограничиваются выделением финансовых средств, 37% - довольствуются наличием квалифицированного персонала (рис. 2)[1].

Незначительное участие руководителей организаций в выработке политики обеспечения безопасности указывает на слабые позиции организаций как субъекта безопасности в определении целей, а также постановке и решений приоритетных задач.

Аналогичная ситуация наблюдается и на предприятиях ОПК РФ.

[1] См.: Выдержки из материалов исследования, проведенного компанией Ernst & Young в области информационной безопасности России и СНГ в 2001 г. доступны на сайте www cnews ru

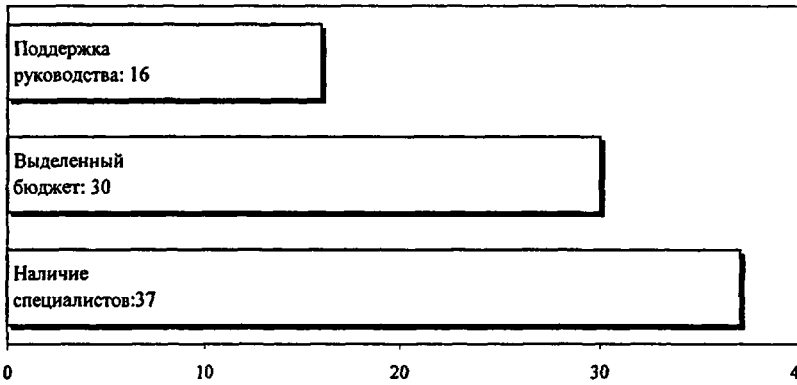

Рис. 2. Отношение респондентов к обеспечению информационной безопасности негосударственных организаций РФ (в %).

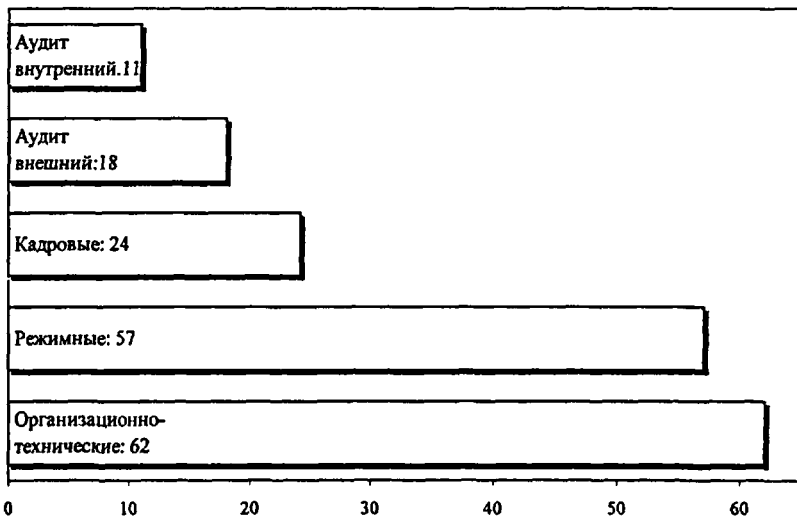

Рис. 3. Отношение респондентов к обеспечению информационной безопасности предприятий ОПК РФ (в %).

Результаты опросов экспертов ОПК, проведенных автором, подтверждают, что, несмотря на общий высокий уровень защищенности информации в

корпоративных информационных системах и сетях, уровень защищенности информации предприятий ОПК снизился (рис.3). Многие руководители предприятий не осознают значимость обеспечения информационной безопасности предприятия, не имеют знаний по защите информации, не выполняют в полной мере нормативные требования и предписания государственных органов, что указывает на слабые позиции предприятия как субъекта безопасности и как следствие слабую защищенность жизненно важных интересов предприятия и государства[1].

Анализ деятельности федеральных органов власти показывает, что в федеральные программы не заложены основные принципы обеспечения информационной безопасности: законность, баланс интересов, взаимная ответственность по обеспечению безопасности, реальность выдвигаемых задач, сочетание централизованного и децентрализованного управления силами и средствами в рамках обеспечения информационной безопасности РФ. В Доктрине информационной безопасности РФ от 09.09.2000 г. не поставлена задача по развитию субъектов безопасности в духе требований информационного общества. Федеральными органами власти и управления по-прежнему применяются устаревшие методы, формы и способы противодействия угрозам безопасности, которые не позволяют достигать поставленных целей и приводящие нередко к недостоверной статистике угроз, не возмещению нанесенного ущерба этими угрозами.

На основании полученных результатов автор делает вывод о неэффективности существующей государственной политике в области обеспечения информационной безопасности РФ. Это обусловлено уже самой деятельностью государственных органов власти, не

[1] См : Приложение № 1 диссертационного исследования «Приоритетные направления деятельности государства по обеспечению информационной безопасности РФ.

сориентированной на развитие субъектов безопасности в контексте ценностной определенности, а также на проведение государственной политики по развитию социальной сферы, на координацию усилий и взаимодействие государственных институтов власти в области обеспечения информационной безопасности РФ.

В связи с этим для достижения соответствующего уровня информационной безопасности РФ автор рекомендует решить следующие задачи по совершенствованию внутреннего механизма функционирования политики обеспечения информационной безопасности РФ:

создание системы нормативно-правовых актов регулирующих отношения между субъектами и объектами деятельности возникающие в области обеспечения информационной безопасности;

организация непосредственной деятельности государственных органов власти и негосударственных организаций по обеспечению информационной безопасности личности, общества и государства, а также эффективное управление этой деятельностью через интересы;

построение системы обеспечения информационной безопасности на базе основополагающих принципов обеспечения безопасности;

разработка механизма выработки политических решений, их исполнения и контроля;

достижение ценностно-ориентационной определенности в отношении представлений о свободе и безопасности личности, общества и государства в сфере информационной деятельности в целях формирования субъектов безопасности.

Решение этих задач возможно в рамках развития государственной системы обеспечения информационной безопасности и формирования негосударственной системы информационной безопасности.

На основе задач, автором определены следующие приоритеты государственной политики в области обеспечения информационной безопасности РФ:

- формирование и развитие субъектов информационной безопасности РФ на базе общепризнанных ценностей российского общества и на основополагающих принципах информационной безопасности;
- совершенствование государственной политики информационной безопасности с учетом конкретных количественно-качественных показателей, отражающих жизненно важные интересы личности, общества и государства;
- образование негосударственной системы страхования информационных рисков, гарантирующей защищенность жизненно важных интересов личности, общества и государства от угроз в информационной сфере.

В заключении диссертации подводятся общие итоги исследования, формулируются научные результаты и основные выводы. Главным из них является вывод о необходимости формирования субъектов информационной безопасности на федеральном, региональном и муниципальном уровнях власти, способных управлять процессом обеспечения информационной безопасности РФ с учетом научно обоснованных приоритетов.

По теме диссертации опубликованы следующие работы:

1. Левин А.А. Тезисы к научно-практической конференции «Проблемы внутренней безопасности России **в** XXI веке» // В сб.: Проблемы внутренней безопасности России в XXI веке / В соавторстве с Дойченко СВ., Дрыновым О.В., Балабановым А.А. / Под. ред. А.В. Возженикова.- М: РАГС, 2001. - 1,5 / 0,5 п.л.

2. Левин А.А. Обеспечение информационной безопасности государственных предприятий и учреждений Российской Федерации // В сб.: Проблемы внутренней безопасности России в XXI веке. — М.: РАГС, 2003. - 0,2 п.л.

3. Левин А.А. Проблемы информационной безопасности России в XXI веке // В сб.: Социальные и гуманитарные науки. (Сер. 4. Государство и право) - М.: РАН ИНИОН, 2002. - № 4. - 0,2 п.л.

4. Левин А.А. Защита интересов личности, общества, государства в информационной сфере // В сб.: Социальные и гуманитарные науки. (Сер. 4. Государство и право) - М.: РАН ИНИОН, 2003. - № 2 - 0,2 п.л.

5. Левин А.А. О политике обеспечения информационной безопасности России // Безопасность. - 2003. - № 1 - 2 (61). - 0,4 п.л.

Автореферат

диссертации на соискание ученой степени
кандидата наук

Левин Александр Алексеевич

Приоритетные направления деятельности
государства по обеспечению информационной
безопасности Российской Федерации
(политологический анализ)

Научный руководитель
Возженников Анатолий Васильевич

Изготовление оригинал-макета
Левин Александр Алексеевич

Подписано в печать 17.05. Тираж 80 экз.

Усл. п.л. 1,2

Российская академия государственной службы
при Президенте Российской Федерации

Отпечатано ОПМГ РАГС. Заказ № 255

119606 Москва, пр-т Вернадского, 84