На правах рукописи

ОСТАПЕНКО ВЕРА СЕРГЕЕВНА

ГОСУДАРСТВЕННАЯ ПОЛИТИКА В ОБЛАСТИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНОВ ИСПОЛНИТЕЛЬНОЙ ВЛАСТИ

(региональный аспект)

Специальность 23.00.02 – политические институты, этнополитическая конфликтология, национальные и политические процессы и технологии

Автореферат
диссертации на соискание ученой степени
кандидата политических наук

Ростов-на-Дону – 2009

Работа выполнена на кафедре политологии и этнополитики Северо-Кавказской академии государственной службы.

Научные руководители: заслуженный деятель науки Российской Федерации, доктор политических наук, профессор **Понеделков Александр Васильевич**

доктор политических наук, профессор **Бусленко Николай Иванович**

Официальные оппоненты: доктор социологических наук, профессор **Щербакова Лидия Ильинична**

кандидат политических наук, доцент **Стариков Александр Георгиевич**

Ведущая организация: Кубанский государственный университет

Защита состоится 4 июля 2009 года в 9-00 часов на заседании диссертационного совета Д 502.008.02 по политическим наукам при Северо-Кавказской академии государственной службы по адресу: 344002, г. Ростов-на-Дону, ул. Пушкинская, 70, аудитория № 514.

С диссертацией можно ознакомиться в библиотеке Северо-Кавказской академии государственной службы.

Автореферат разослан 3 июня 2009 года

Отзывы на автореферат, заверенные печатью, просим присылать по адресу: 344002, г. Ростов-на-Дону, ул. Пушкинская, 70, СКАГС, к. 304.

Ученый секретарь
диссертационного совета Кислицын С.А.

Общая характеристика работы

Актуальность исследования. В условиях глобальных вызовов главным стратегическим национальным ресурсом, определяющим экономическую и оборонную мощь государства, в данном случае – России, являются информация и информационные технологии, от которых в решающей степени зависят все сферы жизнедеятельности российского общества: производство и управление, оборона и энергетика, транспорт и связь, банковское дело и финансы, наука, образование и многие другие. При этом недостаточная защищенность информационных ресурсов приводит к утечке важнейшей политической, экономической, научной, военной информации.

Необходимость улучшения организации работы органов исполнительной власти по реализации основных направлений внутренней и внешней политики государства, определяемых Президентом Российской Федерации, неуклонное возрастание потребностей органов государственного управления в объективной, достоверной и своевременной информации о реальном положении дел в той или иной отрасли, секторе экономики, регионе, городе, предприятии, обусловливает актуализацию процессов информатизации в сфере государственного управления. Информатизация во всех сферах деятельности на базе широкого использования программно-аппаратных средств зарубежного производства, при отсутствии единой централизованной методологии по построению ведомственных и территориальных информационно-коммуникационных систем, привела к бесконтрольному созданию и дублированию информационных ресурсов, появлению множества трудно выявляемых точек доступа к ним. Эти обстоятельства, в условиях хорошо развитых технических средств разведки и широких возможностей, практически официального их использования, а также низкое качество существующих средств защиты, привели к возникновению широкого спектра угроз, формированию нетрадиционных технических и иных каналов утечки информации, равно как и способов несанкционированного доступа к ней.

Актуальность проблемы обеспечения безопасности информации в структурах органов исполнительной власти обусловлена, кроме того, необходимостью принятия эффективных, адекватных политическим задачам, управленческих решений. Во-первых, отметим, что зависимость от информации и информационных технологий становится одним из качественных состояний формирующегося общества. Обладание своевременными, точными, достоверными данными служит чрезвычайно важным фактором эффективности принятия управленческих решений как на государственном уровне, так и на уровне субъектов Федерации. Информация становится стратегической ценностью как государства, так и любой управленческой структуры в системе политического управления. В конечном счете, качество функционирования и безопасность информационной сферы, равно как и состояние правового регулирования

отношений в данной сфере определяют уровень развития государства. Как стратегический ресурс информация требует особого государственного отношения не только в смысле её развития и накопления, но и защиты.

Во-вторых, информационная безопасность, как состояние защищенности интересов личности, общества и государства в информационной сфере, определяет и состояние общественно-политической, экономической, оборонной и иных элементов безопасности государств. Стремительное развитие сферы информационных отношений ставит в прямую зависимость от них все стороны общественной жизни, вызывая в ней глубочайшие качественные перемены. Новые информационные технологии меняют образ жизни людей, конверсируют характер и содержание самих категорий, которыми измеряется социальная (жизненная) активность человека, его общение. Сегодня информационные технологии, интенсивно внедряясь в сферу политической деятельности, бизнес, государственное управление трансформируют характер межличностных отношений в обществе, меняют сами принципы ведения бизнеса, управления в сфере политики и экономики.

В-третьих, обеспечение информационной безопасности сопряжено с вопросами обеспечения технологической безопасности страны. Представляет также значительный интерес рассмотрение проблемы соотношения возможностей средств защиты и средств несанкционированного сбора, обработки и доступа к информационным ресурсам, наличия протоколов взаимодействия пользователей и информации, с учётом степени её важности и секретности, состояния социально-экономической и общественно-политической обстановки в стране и её субъектах. Все это вместе взятое, равно как и научный поиск комплексных мер, средств и методов совершенствования системы информационной безопасности политических структур, повышения управленческого потенциала, главным образом, региональных органов исполнительной власти обусловливает высокую степень актуальности диссертационного исследования.

Степень научной разработанности проблемы. Определению базисных понятий, характеризующих информационное общество в целом, посвящен ряд работ зарубежных авторов, большая часть которых написана в русле концепций постиндустриализма: труды Д.Белла, Т.Стоуньера, Э.Тоффлера, М.Кастельса[1].

---

[1] См.: Белл Д. Социальные рамки информационного общества//Новая технократическая волна на Западе/Под ред. П.С. Гуревича. – М.: Прогресс, 1986.; Стоуньер Т. Информационное богатство: профиль постиндустриальной экономики//Новая технократическая волна на Западе/Под ред. П.С. Гуревича – М.: Прогресс, 1986.; Тоффлер Э. Метаморфозы власти: знание, богатство и сила на пороге XXI века – М., 2003, Тоффлер Э. Третья волна – М., 1999, Тоффлер Э. Шок будущего – М., 2003; Кастельс М. Информационная эпоха: экономика, общество и культура – М.: ГУ – Высшая школа экономики, 2000.

Различные аспекты формирующегося информационного общества в России подробно рассматриваются в работах Г.Т. Артамонова, О.Н. Вершинской, Т.В. Ершовой, В.Л. Иноземцева, И.С. Мелюхина, Д.Н. Пескова, С.Т. Петрова, М.В. Якушева и др.[2]

Неуклонно расширяется диапазон исследований, объектом которых становятся те или иные аспекты обеспечения национальной безопасности России. Здесь отметим работы К.М. Авджяна, О.А. Артюхина, С.А. Олейникова, А.Н. Фролова и др.[3]

Осмыслению информационной безопасности органов исполнительной власти помогают научные труды, исследующие проблемы эффективности государственного управления. Среди них выделим работы А.К. Агапонова, Д.П. Зеркина, В.Г. Игнатова, С.А. Кислицына, А.В. Понеделкова, В.М. Попова, В.М. Радченко, В.А. Сологуба, А.М. Старостина, Л.Г. Швец.

Научное осмысление информационной безопасности как деятельности органов исполнительной власти по защите национальных интересов государства, общества и личности от угроз в информационной сфере значительно усилилось в последнее десятилетие. Можно вести речь о трех конкретных исследовательских и прикладных научных направлениях.

Первое из них – «техническое» – изучает технические аспекты защиты информации в информационных системах и сетях, а также возможности субъектов информационной безопасности противодействовать информационным преступлениям. Здесь следует отметить работы Б.Ю. Анина, В.С. Барсукова, В.А. Галатенко, С.Н.

---

[2] См.: Артамонов Г.Т. О концептуальной базе построения в России информационного общества//Информационное общество. – 1999. – № 3; Вершинская О.Н. Информационно-коммуникационные технологии и общество – М.: Наука, 2007; Ершова Т.В. Российский опыт интеграции в информационное общество//Информационное общество. – 1999. – № 1; Новая постиндустриальная волна на Западе. Антология/Под ред. В.Л. Иноземцева. – М., 1999, Иноземцев В.Л. Современное постиндустриальное общество: природа, противоречия, перспективы: Учебн. пособие для студентов вузов – М., 2000; Мелюхин И.С. Информационное общество: истоки, проблемы, тенденции развития – М., 1999; Песков Д.Н. Интернет в российской политике: утопия и реальность//Полис. – 2002. – № 1; Петров С.Т. На пути к информационному государству//Информационное общество. – 1999. – № 4; Якушев М.В. Информационное общество и правовое регулирование: новые проблемы теории и практики//Информационное общество. – 1999. – № 1.

[3] См.: Авджян К.М. Функционирование системы внутренней безопасности в условиях переходных социально-политических процессов (региональный уровень): дис.… канд. полит. наук: 23.00.02/К.М.Авджян; СКАГС. – Ростов н/Д, 2004; Артюхин О.А. Экологическая составляющая национальной безопасности современной России (региональный аспект): автореф. дис….. канд. полит. наук: 23.00.02/О.А. Артюхин; ГОУ ВПО «СКАГС». – Ростов н/Д, 2006; Олейников С.А. Проблемы национальной безопасности на муниципальном уровне в условиях переходных социально-политических процессов современной России: автореф. дис….. канд. полит. наук: 23.00.02/С.А. Олейников; СКАГС. – Ростов н/Д, 2005; Фролов А.Н. Эффективность национальной безопасности на региональном уровне: критерии и механизмы политического обеспечения: дис.… канд. полит. наук: 23.00.02/А.Н. Фролов; СКАГС. – Ростов н/Д, 2006.

Гриняева, Д.П. Зегжды и А.М. Ивашко, А.В. Петракова, В.А. Петрова, А.Я. Приходько, Ю.В. Романца, А.В. Соколова, М.Ю. Уфимцева, Л.М. Ухлинова, В.Д. Цыганкова, В.И. Ярочкина и др.[4]

Второе направление – «правовое» – анализирует правовые аспекты защиты интересов личности, общества и государства в информационной сфере. К этой группе относятся научные работы А.И. Алексенцева, И.Л. Бачило, В.М. Боера, Н.И. Бусленко, С.Н. Головина, В.Г. Грачева, Т.В. Закупень, В.А. Копылова, В.Н. Крутикова, В.Н. Лопатина, Т.В. Поляковой, Ю.Г. Просвирина, О.А. Степанова, Д.А. Ястребова и др.[5] В

---

[4] См.: Анин Б.Ю. Защита компьютерной информации – СПб.: BHV-Санкт-Петербург, 2000; Барсуков В.С. Современные технологии безопасности: Интегр. подход/Барсуков В.С., Водолазкий В.В. – М.: Нолидж, 2000; Галатенко В.А. Основы информационной безопасности. Курс лекций/Под ред. члена-корр. РАН В.В. Бетелина – М.: Интернет-Университет Информационных Технологий, 2003; Гриняев С.Н. Интеллектуальное противодействие информационному оружию – М.: СИНТЕГ, 1999; Зегжда Д.П. Основы безопасности информационных систем/Зегжда Д.П., Ивашко А.М. – М.: Горячая линия – Телеком, 2007; Петраков А.В. Основы практической защиты информации – М.: Радио и связь, 2000; Петров В.А. Информационная безопасность. Защита информации от несанкционированного доступа в автоматизированных системах/Петров В.А., Пискарев А.С., Шеин А.В. – М.: МИФИ, 1993; Приходько А.Я. Информационная безопасность в событиях и фактах – М.: СИНТЕГ, 2001; Романец Ю.В. Защита информации в компьютерных системах и сетях/Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. – 2-е изд., перераб. и доп. – М.: Радио и связь, 2001; Соколов А.В. Методы информационной защиты объектов и компьютерных сетей/Соколов А.В., Степанюк О.М. – СПб.: Полигон; М.: АСТ, 2000; Уфимцев Ю.С., Ерофеев Е.А. Информационная безопасность России – М.: Экзамен, 2003; Ухлинов Л.М. Управление безопасностью информации в автоматизированных системах – М., 1996; Цыганков В.Д., Лопатин В.Н. Психотронное оружие и безопасность России – М.: СИНТЕГ, 1999; Ярочкин В.И. Информационная безопасность: Учеб. пособие – М.: Междунар. отношения: Летописец, 2000.

[5] См.: Алексенцев А. И. О составе защищаемой информации//Безопасность информационных технологий. – 1999. – № 2; Бачило И.Л. Состояние нормативно-правового обеспечения информационной безопасности// НТИ. – 1995. – Сер.1 – № 8; Бачило И.Л. Право и обеспечение безопасности информации//Вопросы защиты информации. – 2000. – № 3; Боер В.М. Информационно-правовые проблемы безопасности России – Спб: С.-Петерб. гос. акад. аэрокосм. Приборостроения, 1998; Бусленко Н.И. Политико-правовые основы обеспечения информационной безопасности РФ в условиях демократических реформ: автореферат дис.....докт. полит. наук: 23.00.02/Н.И.Бусленко; ФГОУ ВПО СКАГС – Ростов-н/Д., 2003; Головин С.Н. Правовая безопасность международной электронной коммерции//Информационная безопасность России в условиях глобального информационного общества. Сборник материалов летней сессии 5-й Всероссийской конференции «Инфофорум-5» – М., 2003.; Грачев Г.В. Информационно-психологическая безопасность личности: состояние и возможности психологической защиты – М.: Институт психологии РАН, 1999; Закупень Т.В. Основные направления и принципы формирования законодательства в области информации, информатизации и информационной безопасности//Правовая информатика – М., 1997; Копылов В.А. Информационное право – М., 2001; Крутиков В.Н. Развитие и совершенствование отечественной нормативной базы в области информационной безопасности//Бизнес и безопасность в России. – 2004. – № 38; Лопатин В.Н.. Информационная безопасность России: Человек. Общество. Государство – СПб: Фонд «Университет», 2000; Полякова Т.В. Теоретико-правовой анализ законодательства в области обеспечения информационной безопасности Российской Федерации. Автореф. ... дис. канд. юрид. наук. – М., 2002; Просвирин Ю. Г.

большей степени усилия данных авторов оказались сосредоточенными на правовом обеспечении защиты информации, развитии законодательной базы и совершенствовании правоприменительной практики в области информации, информационных технологий и защите информации.

Наконец, третье направление исследований – «социально-политическое» – посвящено политологическим аспектам обеспечения информационной безопасности, а также изучению проблем защиты субъектов информационной безопасности от негативного информационного воздействия. Это научные работы А.В. Возженикова, А.В. Манойло, Ю.Ф. Нуждина, И.Н. Панарина, А.И. Позднякова, В.Д. Попова, Г.Г. Почепцова, А.А. Прохожева, С.П. Расторгуева, Г.Л. Смолян, А.А. Стрельцова, В.Ю. Толстова, В.Н. Цыгичко, Д.С. Черешкина и др.[6]

Столь мощный исследовательский интерес к проблеме информационной безопасности, тем не менее, слабо реализуется в направлении изучения процессов и методов обеспечения информационной безопасности органов исполнительной власти, как фактора повышения эффективности их деятельности. Политологические аспекты обеспечения информационной безопасности органов исполнительной власти практически не изучались в надлежащей полноте, комплексности и историчности. В связи с этим сформулируем цель и задачи настоящего исследования.

Цель исследования - анализ и обобщение имеющейся практики по обеспечению информационной безопасности региональных органов

Информационное законодательство: современное состояние и пути совершенствования – Воронеж: Изд-во Воронежск. гос. ун-та, 2000; Степанов О.А. Теоретико-правовые основы безопасного функционирования и развития информационно-электронных систем. Дис. ... доктора юрид. наук. Академия управления МВД. – М., 2005; Ястребов, Д.А. Правовое обеспечение информационной безопасности: Учеб.-метод. материалы – М.: ПОЛТЕКС, 2002.

[6] См.: Возженников А.В. Национальная безопасность: теория, политика, стратегия – М.: НПО «Модуль», 2000; Нуждин Ю.Ф., Манойло А.В. Информационная война как инструмент внешней агрессии и территориальной экспансии. Учебное пособие – М: НИИПИ, 2000; Поздняков А.И. Обеспечение информационно-психологической безопасности России в условиях глобализации//Безопасность. – 2003. – № 1-2.; Панарин И.Н. Информационно-психологическое обеспечение национальной безопасности России. Дис....докт. полит, наук. – М., 1998; Поздняков А.И. Информационная война за влияние в мире и политическую власть//Власть. – 1996. – № 10.; Попов В.Д. Государственная информационная политика: состояние и проблемы формирования. Массовые информационные процессы в современной России: Очерки/Отв. ред. А.В.Шевченко. – М.: Изд-во РАГС, 2002; Почепцов Г.Г. Информационные войны – М.: Реф-бук, Ваклер, 2000; Прохожев А.А. Информационная безопасность – важнейшая составляющая национальной безопасности современной России – М., 1996; Расторгуев СП. Философия информационной войны – М.: Вузовская книга, 2001;Стрельцов А.А. Обеспечение информационной безопасности России. Теоретические и методологические основы/Под. ред. В.А. Садовничего и В.П. Шерстюка. – М.: МЦНМО, 2002; Толстов В.Ю. Обеспечение информационной безопасности в России стратегиями социального партнерства: автореферат дис....канд. философ. наук: 09.00.11/В.Ю. Толстов; ФГОУ ВПО РГСУ – Ростов н/Д, 2006; Цыгичко В.Н., Смолян Г.Л., Черешкин Д.С. Информационное оружие как геополитический фактор и инструмент силовой политики – М.: ИСА РАН, 1997.

исполнительной власти, определение и обоснование значения информационной безопасности в повышении эффективности процесса принятия управленческих решений; разработка проблемных направлений обеспечения информационной безопасности региональных органов исполнительной власти, поиск оптимальных методов правовой, организационной и технической защиты информации в региональных органах исполнительной власти.

Реализация цели исследования конкретизируется постановкой следующих **основных задач**:

1. Проанализировать теоретико-методологические основы, особенности и проблемы становления информационного общества в современной России.
2. Обосновать необходимость обеспечения информационной безопасности органов исполнительной власти в условиях перехода страны к информационному обществу.
3. Определить основные направления обеспечения информационной безопасности региональных органов исполнительной власти.
4. Выявить показатели эффективности использования информационных ресурсов в деятельности органов исполнительной власти, а также индикаторы угроз информационной безопасности.
5. Определить факторы, препятствующие внедрению и эффективному использованию существующей организационно-правовой и технической базы информационной безопасности в органах исполнительной власти субъектов Южного федерального округа.
6. Установить индикаторы информационной безопасности органов исполнительной власти, а также определить критерии готовности органов исполнительной власти к эффективному внедрению и использованию современных информационно-коммуникационных технологий.
7. Проанализировать и обобщить опыт Администрации Ростовской области по созданию региональной системы защиты информации.

Объектом исследования выступают общественно-политические отношения органов исполнительной власти субъектов Российской Федерации, находящихся в пределах Южного федерального округа, в информационной сфере.

Предметом исследования являются состояние информационной безопасности, её политико-правовая база, основные методы защиты информации в деятельности региональных органов исполнительной власти.

Теоретическая основа исследования представлена общей теорией национальной безопасности, теорией информации, теорией безопасности, теоретическими разработками отечественных и зарубежных ученых в области информации, информационных технологий и информационной безопасности.

Методологической основой диссертации является система как общенаучных, так и специальных методов исследования социально-политических, правовых и иных гуманитарных проблем.

Среди примененных общенаучных методов исследования автор выделяет индуктивный и системный методы. Метод индукции, заключающийся в обобщении и систематизации эмпирического материала, был применен для определения типологии факторов, препятствующих процессу информатизации в региональных органах исполнительной власти, выявления угроз информационной безопасности органов исполнительной власти.

Системный метод позволил нам выявить структурные элементы информационной безопасности в их взаимосвязи. Это дало возможность определить основные принципы обеспечения информационной безопасности региональных органов исполнительной власти, соответствующие современным условиям информационного развития.

Основными специальными методами данного исследования являются исторический метод (изучение процесса становления российского информационного общества в хронологическом порядке), ситуативный метод (учет всех – устойчивых и временных, объективных и субъективных – условий и обстоятельств, создающих информационную безопасность), институциональный метод (анализ исполнительной власти, как политического института), психологический метод (выявление субъектно-объектных механизмов политического взаимодействия в сфере информационной безопасности).

Также в ходе исследования автор использовал метод политического анализа, чтобы раскрыть причины возникновения проблемы обеспечения информационной безопасности в органах исполнительной власти, объяснить ее симптомы и содержание соответствующих фактов, обосновать степень их распространенности, определить динамику и перспективы развития.

Применяемые методы в совокупности позволили, кроме достижения основной цели исследования, выявить основной комплекс проблем информационной безопасности региональных органов исполнительной власти, разработать предложения по совершенствованию методов правовой, организационной и технической защиты информации в процессе принятия управленческих решений.

Источниковую базу исследования составляют Конституция Российской Федерации (1993), новейшее федеральное законодательство, законы РФ, регулирующие деятельность институтов национальной безопасности, информационной безопасности, в частности, Концепция национальной безопасности РФ, Доктрина информационной безопасности РФ, указы Президента РФ, постановления Правительства РФ, а также нормативно-правовые акты субъектов Российской Федерации. В исследовании нашли отражение отдельные международные документы,

регулирующие правовое положение стран-участниц международных объединений, участницей которых выступает Российская Федерация.

Эмпирическую основу диссертации составили результаты традиционного анализа государственных документов в области обеспечения информационной безопасности, статистические данные органов исполнительной власти субъектов Южного федерального округа, а также информационно-аналитические материалы аппарата полномочного представителя Президента Российской Федерации в Южном федеральном округе.

Научная новизна диссертационного исследования заключается в следующем:

1. Проведен анализ и выявлены основные проблемы становления информационного общества в России.

2. Доказана необходимость обеспечения информационной безопасности органов исполнительной власти в условиях перехода России к информационному обществу, основным показателем которого является открытость деятельности органов исполнительной власти перед гражданами.

3. Выделены внутреннее и внешнее направления обеспечения информационной безопасности региональных органов исполнительной власти.

4. Установлены основные показатели эффективности использования информационных ресурсов в деятельности органов исполнительной власти, а также индикаторы угроз информационной безопасности.

5. Выявлены факторы, препятствующие внедрению и эффективному использованию существующей организационно-правовой и технической базы информационной безопасности в органах исполнительной власти субъектов Южного федерального округа.

6. Определены базовые индикаторы информационной безопасности органов исполнительной власти, установлены критерии готовности органов исполнительной власти к эффективному внедрению и использованию современных информационно-коммуникационных технологий.

7. Проанализирован и обобщен опыт Администрации Ростовской области по созданию региональной системы защиты информации.

На защиту выносятся следующие положения:

1. Становление информационного общества в России сдерживают недостаточный объем и низкая эффективность бюджетного финансирования программ и проектов в сфере внедрения информационно-коммуникационных технологий в различные области жизнедеятельности общества; низкие темпы разработки и системного внедрения проектов информатизации органов власти и бюджетных организаций; несовместимость информационных систем органов власти, ограничивающая их взаимодействие; блокирование консервативно

настроенными чиновниками проектов модернизации и использования информационно-коммуникационных технологий в интересах повышения эффективности государственного управления.

2. Необходимость обеспечения информационной безопасности органов исполнительной власти в условиях перехода России к информационному обществу обусловлена тем, что в системе государственного управления обращается множество видов конфиденциальной информации: государственная тайна, служебная информация, коммерческая тайна, персональные данные физических лиц, информация о деятельности юридических лиц, научно-техническая и другие виды информации. Нарушение статуса конфиденциальности обесценивает информацию, поэтому информация должна быть защищена от воздействий, нарушающих ее статус, что и относится к сфере безопасности информации. В то же время механизмы защиты конфиденциальности вступают в противоречие с механизмами обеспечения открытости информации и информационной деятельности органов исполнительной власти перед гражданами, что требует разработки регламентов обобщенного информирования для внешних пользователей.

3. Информационная безопасность органов исполнительной власти представляет собой совокупность мероприятий организационного, технического и правового характера внутреннего и внешнего направлений. Внутреннее направление связано с обеспечением информационной безопасности самих органов исполнительной власти в процессе осуществления ими своих функций. Внешнее направление заключается в обеспечении информационной безопасности региона в целом, что достигается путем повышения эффективности использования информационной инфраструктуры в интересах социально-экономического развития региона.

4. Показателями эффективности использования информационных ресурсов в деятельности органов исполнительной власти являются:

– модернизация системы информационного обеспечения;

– создание элементов электронного правительства, включая обеспечение информационной открытости деятельности органов исполнительной власти;

– развитие систем электронного документооборота;

– расширение набора услуг, предоставляемых в электронной форме;

– привлечение профессионально подготовленных управленческих кадров, способных применять и активно использовать в своей практической деятельности новые информационные технологии.

Выявленными индикаторами угроз информационной безопасности органов исполнительной власти являются разглашение информации, её утечка и несанкционированный доступ к информации, которые могут

привести к негативным последствиям вследствие искажения или хищения информации.

5. Основными факторами, препятствующими внедрению и эффективному использованию существующей организационно-правовой и технической базы информационной безопасности в органах исполнительной власти, являются отсутствие концепций и планов в области информационной безопасности, предусматривающих ситуативный подход, нескоординированность действий федеральных и региональных органов исполнительной власти, отсутствие конкретной нормативно-правовой базы по вопросам информационной безопасности, а также недостаточное число квалифицированных кадров.

6. Индикаторами информационной безопасности органов исполнительной власти являются:

– удовлетворение информационных потребностей органов исполнительной власти, включенных в информационную среду;

– обеспечение безопасности информации, циркулирующей в органах исполнительной власти;

– защита органов исполнительной власти от негативного информационного воздействия.

Основными критериями готовности органов исполнительной власти к эффективному внедрению и использованию современных информационно-коммуникационных технологий являются их организационные, методические, кадровые и финансовые возможности.

7. Опыт Администрации Ростовской области, которая занимается созданием региональной системы защиты информации практически с 1995 года, уникален по своей разнонаправленности и может быть использован другими органами исполнительной власти в целях повышения эффективности своей работы.

Практическая значимость исследования заключается в том, что полученные результаты исследования могут быть использованы: при разработке общегосударственной Концепции обеспечения информационной безопасности органов исполнительной власти; в практической деятельности органов исполнительной власти по организации нормативно-правовой и технической защиты информации, по координации работ по обеспечению информационной безопасности; при разработке проектов региональных систем защиты информации, которые имеют своей целью повышение эффективности работы региональных органов исполнительной власти; в научно-практической деятельности, а также в учебных программах обучения студентов, повышения квалификации государственных гражданских служащих.

Апробация результатов исследования. Основные положения и результаты диссертационного исследования докладывались и обсуждались на международной научно-практической конференции «Элиты и будущее России: взгляд из регионов», Ростов-на-Дону, 12-13 октября 2007 года, межрегиональной научно-практической

междисциплинарной конференции студентов и молодых ученых Юга России «Молодежь как инновационный ресурс развития современного российского общества», Ростов-на-Дону, 5-6 ноября 2008 года, научно-практической конференции «Государственная политика по формированию резерва управленческих кадров на региональном уровне: опыт, проблемы, пути решения», Ростов-на-Дону, 27-28 февраля 2009 года, опубликованы в 10 статьях и научных работах общим объёмом 3,5 п.л.

Структура диссертации. Работа состоит из введения, трёх глав, заключения общим объёмом 151 страница, списка литературы из 118 источников и 4 приложений.

Основное содержание диссертации

Во **введении** дается общая характеристика диссертационной работы, а именно: обосновывается актуальность темы исследования, раскрывается степень ее научной разработанности, формулируется основная цель и задачи исследования, определяются объект и предмет, а также формулируются теоретическая и методологическая основы, эмпирическая база.

В **главе 1. Теоретико-методологические основы информационной безопасности в парадигме современного информационного общества** раскрывается теоретическое и методологическое обоснование значения информационной безопасности в жизнедеятельности личности, общества, государства с точки зрения перехода к информационному обществу. Основное внимание уделено рассмотрению теории информационного общества, полагающей главным фактором развития производство и использование научно-технической и другой информации. Данная теория является разновидностью теории постиндустриального общества, основу которой заложили Э.Тоффлер, Д.Белл, З.Бжезинский. Именно в их фундаментальных трудах, вышедших в 70-80-е гг., были сформулированы основные черты этого общества, которое Э.Тоффлер назвал «третьей волной»[7].

Под информационным обществом понимается общество, в котором информация, знания, информационные услуги и все отрасли, связанные с их производством, растут более быстрыми темпами, являются источником новых рабочих мест, становятся доминирующими в экономическом развитии. В настоящее время в России проблема формирования информационного общества рассматривается как необходимое условие её устойчивого развития, полноценной интеграции в мировое сообщество. По мнению автора, на сегодняшний день мы сильно отстаем в этой области, хотя в последнее время темпы информатизации растут достаточно быстро. С целью сокращения отставания России от развитых стран в уровне развития, распространения и эффективного использования информационно-коммуникационных технологий принят и реализуется ряд основополагающих документов. Среди них автор выделяет Концепцию

[7] См.: Тоффлер Э. Третья волна – М., 2004.

государственной информационной политики, Доктрину информационной безопасности Российской Федерации, Федеральную целевую программу «Электронная Россия (2002-2010 годы)», Стратегию развития информационного общества в России.

Концепция государственной информационной политики была разработана в 1998 году.[8] Она направлена на создание основ для решения таких жизненно важных задач, как формирование единого информационного пространства России, развитие сферы информационных услуг, совершенствование правового поля регулирования происходящих информационных процессов, ее интеграции в мировое информационное пространство. При этом особое внимание уделяется обеспечению информационной безопасности личности, общества и государства.

Утверждение *Доктрины информационной безопасности Российской Федерации* оказалось существенным шагом на пути дальнейшей информатизации российского общества, стала концептуальным документом в области информационной безопасности. Доктрина служит основой для формирования государственной политики в области обеспечения информационной безопасности и представляет собой совокупность официальных взглядов на цели, задачи, принципы и основные направления обеспечения информационной безопасности Российской Федерации[9].

Постановлением Правительства Российской Федерации в январе 2002 года утверждена *Федеральная целевая программа (ФЦП) «Электронная Россия (2002-2010 годы)».* Её разработка стала существенным шагом в повышении политического внимания к проблемам информатизации, концентрации национальных усилий на информационно-коммуникационном направлении и координации государственной деятельности в данной сфере.

Основным документом в области формирования информационного общества в России является утвержденная Президентом Российской Федерации Д.А. Медведевым «*Стратегия развития информационного общества в России*»[10] 7 февраля 2008 года. Целью формирования и развития информационного общества в Российской Федерации названо повышение качества жизни граждан, обеспечение конкурентоспособности России, развитие экономической, социально-политической, культурной и духовной сфер жизни общества, совершенствование системы

---

[8] Артамонов Г.Т., Кристальный Б.В., Курносов И.Н. и др. О концептуальной базе построения в России информационного общества//Информационное общество – 1999. – № 9. С.17-19.

[9] См.: Доктрина информационной безопасности Российской Федерации. Утверждена поручением Президента Российской Федерации от 9 сентября 2000 года № Пр-1897//Российская газета, 2000, 28 сент.

[10] Стратегия развития информационного общества в Российской Федерации. Утверждена поручением Президента Российской Федерации от 7 февраля 2008 года № Пр-212//Российская газета, 2008, 16 февр.

государственного управления на основе использования информационных и телекоммуникационных технологий.

Далее отметим, что широкое внедрение компьютерных технологий во все сферы жизни современного общества повысили его уязвимость для противоправных действий и вызвали стремительный рост компьютерных преступлений. Выход в глобальную сеть Интернет влечет за собой угрозы информационной безопасности национальных компьютерных систем. Прежде всего, это несанкционированный доступ к информационным ресурсам, а также их возможное разрушение. Использование импортных информационных технологий в автоматизированных системах управления различными производствами, транспортом и т.п. без принятия соответствующих мер по обеспечению информационной безопасности создает реальные угрозы национальной безопасности России.

Существующие в научной литературе понятия информационной безопасности классифицируются в две группы. В первой группе понятий информационная безопасность связывается с защитой информации, информационных ресурсов, личности, общества и государства от негативного информационного воздействия, которое может привести к искажению информации, изменению информационного мышления пользователей информации и, как следствие, к непредсказуемым социальным или политическим процессам.

Вторая группа объединяет научно-технические свойства информационной безопасности, акцентирует внимание на угрозах информационной безопасности, возникающих вследствие информационной неопределенности, когда потребитель (личность, общество или государство) по каким-либо причинам не может воспользоваться информацией, циркулирующей в информационном пространстве.

Особое внимание автор уделяет рассмотрению угроз информационной безопасности и их классификации. Несмотря на все многообразие определений угроз информационной безопасности, практически все они отражают одну и ту же суть. Под угрозой понимается опасность (существующая реально или потенциально) совершения какого-либо деяния (действия или бездействия), направленного на нарушение основных свойств информации: конфиденциальности, целостности, доступности. Раскрывая виды возможных нарушений основных свойств информации, практически все исследователи приводят один и тот же перечень: к угрозам нарушения конфиденциальности информации относят хищение (копирование) и утечку информации; к угрозам доступности – блокирование информации; к угрозам целостности – модификацию

(искажение информации), отрицание подлинности информации или навязывание ложной информации.[11]

Угрозами информационной безопасности процесса принятия решений являются разглашение, утечка и несанкционированный доступ, которые могут привести к негативным последствиям вследствие искажения или хищения информации. Системный подход к информационной безопасности требует определения как её содержания и опасностей, так и принципов её обеспечения. Исходя из определения информационной безопасности, основными принципами её обеспечения, по мнению автора, могут быть принципы: законности, обоснованности, своевременности, прогностичности и устойчивости.

Таким образом, информационная безопасность трактуется автором, как состояние защищенности информационных ресурсов, технологий их формирования и использования, а также прав субъектов информационных отношений от внутренних и внешних воздействий различного характера, направленных на нарушение конфиденциальности, целостности или доступности информации, обеспечиваемое комплексным применением принципов законности, обоснованности, своевременности, прогностичности и устойчивости.

Далее автор подходит к рассмотрению информационной безопасности с точки зрения субъектно-объектного подхода, который оформился в 60-70-е гг. XX в. Он связан с трактовкой вопроса об отношении субъективного к объективному, мышления к бытию, как основного вопроса философии[12], и является теоретической базой, на которой развивается большинство научных направлений. В настоящее время сторонники этого подхода рассматривают вопрос об отношении субъекта к объекту в качестве необходимого компонента (аспекта) любой философской проблемы. Данный подход основан на изучении двух категорий – «объекта» и «субъекта», взаимодействие которых происходит в окружающей их среде.

Применительно к информационной безопасности специфика субъектно-объектных отношений устанавливается благодаря особенностям, присущим каждой из рассматриваемых категорий, т.е. объекта информационной безопасности и субъекта информационной безопасности. Объект информационной безопасности – это всё то, что терпит ущерб в результате объектно-субъектных отношений, а субъект информационной безопасности – всё то, что наносит ущерб. К объектам и субъектам информационной безопасности относятся любые системы (социальные, природные, технические и т.п.), которые обладают определенной совокупностью свойств. Различие между ними заключается

---

[11] См.: Пархоменко Н., Яковлев С., Пархоменко П., Мисник Н. Угрозы информационной безопасности. Новые реалии и адекватность классификации//Защита информации. – 2003. – Конфидент № 6. С.12-18.

[12] См.: Перминов В.Я. Философия как метод//Вестник Московского университета. Серия 7. Философия. – 1997. – № 5. С.3-25.

в том, что объекту информационной безопасности принадлежат привлекательные для субъекта информационной безопасности свойства, а субъект информационной безопасности обладает способностью (т.е. свойством) к уничтожению (повреждению, изъятию, видоизменению, завладению и т.п.) привлекательных свойств объекта информационной безопасности. Объект безопасности противостоит субъекту безопасности.

Объектом информационной безопасности являются информационные ресурсы, технологии их формирования и использования, а также информационная инфраструктура, используемая для создания информации, ее сбора, обработки, накопления, хранения, распространения и предоставления потребителям. Субъектом информационной безопасности являются личность, группа людей, организации, органы государственной власти или отдельные должностные лица, нарушающие своими действиями конфиденциальность, целостность или доступность информации, т.е. приносящие ущерб объекту информационной безопасности. В структуре субъектно-объектных отношений в системе информационной безопасности автор отводит особое место положению человека. Благодаря человеку информационные системы приобретают социальные качества и являются источником повышенной опасности. Человек в них выступает как объект и субъект отношений. В системе информационной безопасности он не только вносит элемент упорядочения и организации, но и способен дезорганизовать, повредить или ухудшить состояние информационной инфраструктуры.

Глава 2. Информатизация и защита информации в органах исполнительной власти в условиях перехода к информационному обществу посвящена анализу основных функций исполнительной власти как политического института и обоснованию информационной безопасности как фактора повышения эффективности процесса управления регионом.

Автор рассматривает исполнительную власть как особый политический институт, через который государство осуществляет свои функции по руководству и регулированию общественными отношениями. Органы исполнительной власти осуществляют руководство административно – политической, социально-культурной и, в известной степени, производственно-трудовой деятельностью во всех её многообразных проявлениях, что неизбежно придает этой деятельности в силу её постоянства профессиональный характер. Важным признаком исполнительной власти являются её широкие возможности использовать административное принуждение для решения стоящих перед ней задач. Институт административного принуждения – необходимый атрибут данной власти. По мнению автора, административное принуждение – это не бесконтрольное насилие, а основанная на законе и обусловленная им деятельность органов исполнительной власти, направленная на охрану общественного порядка, безопасности граждан, их прав и интересов.

Особенность исполнительной власти выражается в существовании двух уровней ее функций – основном и вспомогательном. Основной уровень охватывает функции, имеющие глобальное значение для жизни общества и вытекающие из субстанциональной природы этой власти. Исполнительная власть гораздо полнее, чем законодательная, представляет единство, сущность, функциональную направленность государства, а потому основное назначение государства – охранять внутренний и внешний мир общества, обеспечивать его благосостояние – реально и содержательно воплощаются в ее функциях.

Осуществляя практическую деятельность по организации социальной жизни общества, исполнительная власть для эффективной реализации основных функций нуждается в наличии полномочий, которые давали бы ей возможность собственными действиями осуществлять правовое регулирование, правоприменительную и юрисдикционную деятельность. Поэтому государство наделяет исполнительную власть полномочиями, образующими вспомогательный уровень её функций. Функции данного ряда имеют инструментальный характер и направлены на обслуживание каждой из основных функций. Функции исполнительной власти второго уровня – это нормотворчество, правоприменение, юрисдикция. Они используются как организационно-технические средства реализации основных функций. Универсальность исполнительной власти проявляется также в том, что она охватывает все важнейшие сферы и отрасли общественной жизни, географически распространяется на все регионы и территории страны, подразделяясь по вертикали на федеральный, региональный и муниципальный уровни.

Мы полагаем, что сущность исполнительной власти заключается в оперативном управлении обществом и отдельными его сферами на основе данных ей полномочий через процесс принятия управленческих решений, по типу которых, способу разработки, уровню участия различных субъектов (в том числе массовых) можно судить о существенных признаках общественно-политической системы. Управленческие решения являются основным инструментом реализации управленческих воздействий. Поэтому и эффективность управленческой деятельности напрямую зависит от способности принимать и реализовывать эти решения. Особое значение имеет деятельность органов исполнительной власти, управленческое воздействие которых осуществляется посредством принимаемых правовых актов (управленческих решений) – постановлений, распоряжений. От качества подготовки, реализации и контроля исполнения управленческих решений во многом зависит эффективность деятельности органов исполнительной власти. Соответственно вырастает цена оптимальности принимаемых решений.

Рассмотрим необходимость детальной разработки концепции обеспечения информационной безопасности органов исполнительной власти в целях повышения эффективности их деятельности. Содержание исполнительной власти составляет исполнительно-распорядительная

деятельность по непосредственному управлению всеми общественно значимыми сторонами жизни государства. Одна из главных целей государственного управления состоит в том, чтобы на базе собранных исходных данных получить вторичную, обработанную информацию, которая служит основой для принятия управленческих решений. Рост объема информации, циркулирующей в органах исполнительной власти, интенсивности и динамичности информационных потоков, с одной стороны, и отсутствие отработанных способов информационного обеспечения процесса управления с другой, формируют противоречие между необходимостью максимального использования растущего объема информации при принятии управленческих решений и реальным состоянием информационного обеспечения управленческой деятельности.

Заметим, что в современном мире информация имеет прямое отношение к политическим процессам. «Процессы сбора, накопления, переработки и распространения информации есть необходимое условие существующих структур управления, осуществления эффективных политических воздействий, решения масштабных экономических задач»[13]. Если государственный служащий – основа государственного управления, авторитет власти, то информация – её сила, главное богатство экономики. Управленец и управленческая информация представляют единое целое, они взаимосвязаны. Действительно, эффективность управленческой информации зависит от степени влияния на нее уровня интеллекта, компетентности, профессионализма пользователя – государственного служащего, свойств и качеств самой информационной системы, используемой при подготовке и принятии управленческих решений. Управленческая информация это не только простое средство общения, взаимодействия, жизнеобеспечения, но и свобода принимать решения, это товар и деньги. Это сила и инструмент власти.

Управленческая информация как основа информационного обеспечения представляет собой элемент социальной информации, выделенный из её общего массива по критериям причастности к обслуживанию государственно-управленческих процессов формирования и реализации управляющих воздействий. Особую социальную значимость в деятельности органов исполнительной власти представляет феномен качественно новой управленческой информации. Смысл её новизны не в содержательном аспекте, а в том, как происходит процесс её сбора, накопления, обработки, передачи, хранения и представления. Применение и использование её в органах исполнительной власти позволяет перейти на более высокий уровень выработки и принятия управленческих решений. Автор рассматривает информационную безопасность органов исполнительной власти через совокупность таких индикаторов, как

---

[13] Бусленко Н.И. Политико-правовые основы обеспечения информационной безопасности РФ в условиях демократических реформ: автореферат дис.....докт. полит. наук: 23.00.02/Н.И.Бусленко; ФГОУ ВПО СКАГС – Ростов-н/Д., 2003. С.5.

удовлетворение информационных потребностей, обеспечение безопасности информации и защита от негативного информационного воздействия, которые выступают фактором повышения эффективности принимаемых управленческих решений на основе соблюдения требований полноты, достоверности и своевременности информации.

Анализ деятельности органов исполнительной власти Южного федерального округа позволил выделить в данной работе основные принципы обеспечения их информационной безопасности, которые направлены на повышение эффективности процесса принятия управленческих решений на основе имеющейся информации о социально-политическом и экономическом состоянии в регионах. Становится очевидной необходимость разработки положения о защите информации в региональном органе исполнительной власти, т.е. разработки нормативно-правового документа, направленного на обеспечение информационной безопасности. Руководствуясь результатами, полученными в ходе диссертационного исследования, автор разработала проект Типового положения о защите информации в органе исполнительной власти субъекта Российской Федерации. Подобный документ должен быть принят на федеральном уровне и послужить основой для разработки и принятия в региональных органах исполнительной власти соответствующих нормативных актов.

Глава 3. Информационная безопасность органов исполнительной власти в субъектах Южного федерального округа (состояние, методы совершенствования) посвящена детальному изучению состоянию дел в сфере информационной безопасности в субъектах Южного федерального округа, а также разработке рекомендаций по данной проблеме.

В главе раскрывается состояние процесса информатизации и информационной безопасности в органах исполнительной власти Южного федерального округа. Автором был проведен анализ реализации основных положений Доктрины информационной безопасности Российской Федерации в регионах Южного федерального округа; нормативно-правовых актов субъектов Российской Федерации по вопросам обеспечения информационной безопасности.

Защита информации является неотъемлемой составной частью основной деятельности органов исполнительной власти, она обеспечивается проведением комплекса правовых, организационных и технических мероприятий, направленных на предотвращение или преодоление конкретных угроз безопасности информации в зависимости от условий деятельности и решаемых задач. Автор выделяет основные факторы, определяющие необходимость повышения внимания к вопросам защиты информации конкретно в Южном федеральном округе.

Так, например, с 2002 года в десяти субъектах Российской Федерации, находящихся в пределах Южного федерального округа, выполнялись работы по реализации, в общей сложности, четырнадцати

мероприятий ФЦП «Электронная Россия (2002-2010 годы)», а также пяти мероприятий, содержащих задания по внедрению информационно-коммуникационных технологий. По семь мероприятий в сфере информационно-коммуникационных технологий реализовывалось в Краснодарском крае и Волгоградской области. Пять мероприятий – в Ставропольском крае. Четыре мероприятия – в Астраханской области. По два мероприятия ФЦП «Электронная Россия» реализовывались в Ростовской области и Карачаево-Черкесской Республике. В республиках Калмыкия, Ингушетия, Дагестан и Северная Осетия-Алания реализовывалось по одному мероприятию в сфере информационно-коммуникационных технологий. Многие принимаемые решения в рамках реализации ФЦП «Электронная Россия (2002-2010 годы)» в целях создания информационной инфраструктуры субъектов Российской Федерации и в целом Южного федерального округа не достигают поставленных целей. Основными причинами этого являются нескоординированность действий федеральных и региональных структур, а также недостаток финансирования. На практике не сложилось единого координатора процессов внедрения и развития информационно-коммуникационных систем в рамках соответствующих Программ.

Тем не менее, в настоящее время в округе создана достаточно разветвленная телекоммуникационная оптоволоконная сеть. В Ставропольском и Краснодарском краях и Ростовской области действуют замкнутые оптоволоконные линии, позволяющие реально приступить к созданию современных сетей передачи данных. В Республике Северная Осетия – Алания, Кабардино-Балкарской Республике, Астраханской области более 90% каналов связи между районными центрами и центрами указанных субъектов являются цифровыми. В Волгоградской области и республиках Дагестан и Ингушетия ведутся работы по созданию региональных сетей управления и передачи данных, в которых предусмотрено подключение как крупных федеральных структур, так и отдельных пользователей. Предусмотрено наличие шлюзов для подключения внешних сетей. Строительство данной сети в Волгоградской области планируется закончить в 2009 году.

В Южном федеральном округе получили развитие инициативы по внедрению перспективных разработок с использованием информационных технологий в сфере представления пакета «электронных» услуг для организаций и населения (в Краснодарском крае, Ростовской и Волгоградской областях реализуется система передачи налоговых деклараций по сети Интернет). Данная система выведена на стадию промышленной эксплуатации. Завершен проект по созданию автоматизированной системы управления органов записи актов гражданского состояния Ставропольского края. Данный проект имеет потенциальные возможности перерасти в проект масштаба Южного федерального округа.

Отметим, что информационные системы органов государственной власти большинства субъектов Южного федерального округа (как и Российской Федерации в целом) разрознены технологически и развиваются самостоятельно с применением разных операционных систем и аппаратных платформ, без согласования форматов хранения, передачи и обработки данных. Устранение указанных проблем возможно путем разработки общегосударственной концепции обеспечения информационной безопасности органов исполнительной власти. Такая концепция позволит обеспечить необходимую эффективность и согласованность мероприятий в сфере информатизации органов исполнительной власти, проводимых субъектами Российской Федерации, в рамках федеральных целевых программ, содержащих задания по информационно-коммуникационным технологиям, а также выйти на достаточный уровень информационной безопасности в деятельности органов исполнительной власти.

В работе предпринят анализ основных проблем обеспечения информационной безопасности органов исполнительной власти Ростовской области и на этой основе предложены конкретные меры по их разрешению.

В частности отмечается, что Администрацией Ростовской области уделяется большое внимание вопросам информатизации органов исполнительной власти области. Так, постановлением Администрации Ростовской области от 3 марта 2003 года № 116 «О создании Совета по информационно-коммуникационным технологиям при Администрации Ростовской области»[14] утверждено Положение о Совете, который является рабочим органом Администрации Ростовской области в части реализации основных мероприятий Федеральной целевой программы «Электронная Россия (2002-2010 годы)» на территории Ростовской области.

Обеспечение информационной безопасности органов исполнительной власти Ростовской области, а также решение проблемы доступа граждан к информации об их деятельности являются одними из важнейших направлений работы Администрации области. В соответствии с постановлением Администрации Ростовской области от 5 мая 2003 года № 216[15] и распоряжением Администрации Ростовской области от 4 мая 2006 года № 168[16] в Ростовской области для информирования населения

---

[14] Постановление Администрации Ростовской области от 3 марта 2003 года № 116 «О создании Совета по информационно-коммуникационным технологиям при Администрации Ростовской области»//Источник: справочно-правовая система «КонсультантПлюс-Регион».

[15] Постановление Администрации Ростовской области от 5 мая 2003 года № 216 «Об обеспечении доступа к информации о деятельности Администрации Ростовской области и областных органов исполнительной власти»//Источник: справочно-правовая система «КонсультантПлюс-Регион».

[16] Распоряжение Администрации Ростовской области от 4 мая 2006 года № 168 «О предоставлении органами исполнительной власти Ростовской области отдельных информационных материалов для официального опубликования»//Источник: справочно-правовая система «КонсультантПлюс-Регион».

создан корпоративный портал www.donland.ru, на котором регулярно публикуется информация о деятельности Администрации и органов исполнительной власти Ростовской области.

Постановлением Главы Администрации Ростовской области от 27 июля 1995 г. № 186[17] создан Совет по вопросам защиты информации при Главе Администрации (Губернаторе) области. Основными функциями данного Совета являются организация и координация работ по вопросам защиты информации в Администрации Ростовской области, областных органах исполнительной власти, администрациях муниципальных образований, взаимодействие и согласование соответствующих мероприятий с Федеральной службой по техническому и экспортному контролю, Федеральной службой безопасности Российской Федерации, Министерством внутренних дел Российской Федерации. С 1995 года Администрация Ростовской области занимается созданием региональной системы защиты информации, которая имеет своей целью повышение эффективности работы органов исполнительной власти. Создан механизм решения задач по определенным направлениям. Можно утверждать, что областной администрацией созданы все необходимые институты региональной системы защиты информации на территории Ростовской области.

Однако для продолжения успешно проводимой в области работы требуется сделать еще многое. Анализ региональной системы защиты информации в Ростовской области показывает, что на территории Ростовской области представлен довольно широкий круг предприятий, занимающихся оказанием услуг в области защиты информации, лицензирования организаций и предприятий на право проведения работ в области защиты информации, аттестации объектов информатизации по требованиям защиты информации, сертификации средств защиты информации по требованиям информационной безопасности, а также организации научной и научно-технической работы в области информационной безопасности. Всё это вместе взято позволяет областным органам исполнительной власти привлекать организации различных форм собственности к оказанию услуг по разработке программ информационной безопасности, как самого органа, так и региона в целом. Администрация Ростовской области целенаправленно создает в регионе такую систему обеспечения защиты информации и информационных ресурсов, которая не позволит нарушать процесс государственного управления путем уничтожения, хищения или разглашения конфиденциальной информации.

В **заключении** диссертации сформулированы основные результаты исследования. Сделаны выводы, даны некоторые рекомендации по

---

[17] Постановление Главы Администрации Ростовской области от 27 июля 1995 года № 186 «О совершенствовании системы защиты информации в Ростовской области»//Источник: справочно-правовая система «КонсультантПлюс-Регион».

решению прикладных задач в сфере обеспечения информационной безопасности органов исполнительной власти субъектов Российской Федерации.

По теме диссертации автором опубликованы следующие работы:

1. Остапенко В.С. Региональная система защиты информации в Ростовской области//Власть. – №6. – 2009. 0,8 п.л. (ведущий журнал)

2. Остапенко В.С. Информационная безопасность взаимодействия федеральных и региональных административных элит//Элиты и будущее России: взгляд из регионов (выпуск второй). Материалы международной научно-практической конференции. Ростов-на-Дону, 12-13 октября 2007 года – Ростов-на-Дону: Изд-во СКАГС, 2007. 0,2 п.л.

3. Остапенко В.С. Проблема информатизации органов исполнительной власти//Актуальные проблемы совершенствования экономико-правовых и социально-политических сфер общества в современной России. Аспирантский сборник. – Ростов-на-Дону: Изд-во СКАГС, 2008. 0,25 п.л.

4. Остапенко В.С. Проблемы обеспечения информационной безопасности в сфере государственного управления//Актуальные проблемы совершенствования экономико-правовых и социально-политических сфер общества в современной России. Аспирантский сборник. – Ростов-на-Дону: Изд-во СКАГС, 2008. 0,25 п.л.

5. Остапенко В.С. Роль молодежи в формировании информационного общества в России//Молодежь как инновационный ресурс развития современного российского общества. Сборник тезисов докладов межрегиональной научно-практической междисциплинарной конференции студентов и молодых ученых Юга России. Ростов-на-Дону, 5-6 ноября 2008 года – Ростов-на-Дону: Изд-во СКАГС, 2008. 0,2 п.л.

6. Остапенко В.С. Информационная безопасность процесса формирования резерва управленческих кадров//Государственная политика по формированию резерва управленческих кадров на региональном уровне: опыт, проблемы, пути решения. Материалы межрегиональной научно-практической конференции. Ростов-на-Дону, 27-28 февраля 2009 года – Ростов-на-Дону: Изд-во СКАГС, 2009. 0,25 п.л.

7. Остапенко В.С. Политический аспект информационной безопасности государственного управления//Политическая наука на Юге России: становление, современное состояние и основные направления развития. Материалы межрегиональной научно-практической конференции. Ростов-на-Дону, 11-12 марта 2009 г. – Ростов-на-Дону: Изд-во СКАГС, 2009. 0,25 п.л.

8. Остапенко В.С. Проблемы защиты информации в органах исполнительной власти Южного федерального округа//Аспирантский сборник. – Ростов-на-Дону: Изд-во СКАГС, 2009. 0,5 п.л.

9. Остапенко В.С., Бусленко Н.И. Информационная безопасность Южного федерального округа// Аспирантский сборник. – Ростов-на-Дону: Изд-во СКАГС, 2009. 0,45 п.л.

10. Остапенко В.С. Информационная безопасность региональных органов исполнительной власти//Государственное и муниципальное управление. Ученые записки СКАГС. – №1 . – 2009. 0,6 п.л.

Подписано в печать 27.05.2009. Усл. п.л. 1,3
Тираж 100 экз. Заказ № 21/5
Ризограф СКАГС. 344002, г.Ростов-на-Дону, ул.Пушкинская, 70