На правах рукописи

Крылов Григорий Олегович

МЕЖДУНАРОДНЫЙ ОПЫТ ПРАВОВОГО РЕГУЛИРОВАНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ЕГО ПРИМЕНЕНИЕ В РОССИЙСКОЙ ФЕДЕРАЦИИ

Специальность 05.13.19 –
методы и системы защиты информации,
информационная безопасность

Автореферат
диссертации на соискание ученой степени
кандидата юридических наук

МОСКВА
2007

Диссертация выполнена на кафедре компьютерного права факультета информационной безопасности Государственного образовательного учреждения высшего профессионального образования Московском инженерно-физическом институте (государственном университете).

Научный руководитель: доктор юридических наук, профессор Морозов Андрей Витальевич

Официальные оппоненты: доктор юридических наук, профессор Стрельцов Анатолий Александрович

доктор юридических наук, профессор Соковых Юрий Юрьевич

Ведущая организация:
Военный университет Министерства обороны Российской Федерации

Защита диссертации состоится 21 мая 2007г. в 16.00 часов на заседании диссертационного Совета ДМ 212.130.08 в МИФИ по адресу: 115409,г. Москва, Каширское шоссе, д. 31, в конференц-зале главного корпуса

С диссертацией можно ознакомиться в библиотеке МИФИ.

Автореферат разослан ____ апреля 2007г.

Просим принять участие в работе совета или прислать отзыв в одном экземпляре, заверенный печатью организации.

Ученый секретарь
диссертационного совета Горбатов В.С.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы исследования. На протяжении веков достижения естественно-научной культуры порождали проблемы гуманитарной культуры. Техника, будучи усилителем способностей человека, всегда бросала вызов праву, ибо использовалась не только во благо, но и во вред личности, обществу и государству. Единство и борьба противоположностей двух культур особенно усиливается при переходе человечества от эпохи усилителей физических способностей человека в энергетической сфере к эпохе усилителей умственных способностей в информационной сфере. Такими усилителями, как известно, являются средства вычислительной техники и связи, которые существенно меняют пространственно-временные характеристики общественных отношений и порождают новые, ранее неизвестные виды девиантных отношений. Господствующей социальной группой в обществе становятся владельцы информации и ноу-хау технологий, общество трансформируется из постиндустриального в информационное. Изменяется геополитическое информационное противоборство государств, которое все чаще принимает форму планомерных информационных операций под прикрытием принципа свободы информации.

Нынешний этап развития информационных технологий характеризуется возможностью массированного информационного воздействия на индивидуальное и общественное сознание вплоть до проведения крупномасштабных информационных войн, в результате чего неизбежным противовесом принципу свободы информации становится принцип информационной безопасности (ИБ).

Этот принцип обусловлен глобальной информационной революцией, стремительным развитием и повсеместным внедрением новейших информационных технологий и глобальных средств телекоммуникаций. Проникая во все сферы жизнедеятельности государств, информационная революция расширяет возможности развития международного сотрудничества, формирует планетарное информационное пространство, в котором информация приобретает свойства ценнейшего элемента национального достояния, его стратегического ресурса.

Вместе с тем, становится очевидным, что наряду с положительными моментами такого процесса создается и реальная угроза использования достижений в информационной сфере в целях, не совместимых с задачами поддержания мировой стабильности и безопасности, соблюдения принципов суверенного равенства государств, мирного урегулирования споров и конфликтов, неприменения силы, невмешательства во внутренние дела, уважения прав и свобод человека. Опасным источником угроз является растущая отечественная и международная компьютерная преступность.

Мировое сообщество признало международную информационную безопасность как глобальную проблему, как необходимое условие существования человеческого сообщества.

В этой связи требуется выработка общих принципов и общего понимания всего комплекса проблем, связанных с информационной безопасностью, начиная с понятийного аппарата, научных и методических концепций и кончая практическим решением стоящих задач.

За последние годы в Российской Федерации начато формирование нормативного правового обеспечения информационной безопасности. Приняты федеральные законы от 27.12.2002 № 184-ФЗ «О техническом регулировании»[1] и от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»[2]. Разработаны Основные направления нормативного правового обеспечения информационной безопасности Российской Федерации, одобренные Межведомственной комиссией Совета Безопасности Российской Федерации по информационной безопасности 27 ноября 2001г. № 4.1.

Однако имеющаяся в России законодательная база не в полной мере отражает потребности обеспечения информационной безопасности

Системная работа в сфере правового обеспечения информационной безопасности требует научного обоснования дальнейшей разработки таких нормативных актов, в которых бы в полной мере были учтены международные принципы и нормы, направленные на укрепление международной информационной безопасности, и вместе с тем максимально учитывались бы национальные интересы. В связи с изложенным тема исследования представляется актуальной.

Цель диссертационного исследования заключалась в обобщении международного опыта правового регулирования информационной безопасности и в обосновании концептуальных положений системы нормативного регулирования в сфере практического обеспечения информационной безопасности кредитных организаций России.

Для достижения сформулированной цели в работе поставлены следующие **задачи:**

1.Исследовать понятийный аппарат, применяемый в отечественном и зарубежном правовом обеспечении информационной безопасности, с учетом состояния и перспектив развития информационных операций, как источника крупномасштабных массированных информационных угроз;

2.Систематизировать международные правовые нормы в сфере информационной безопасности и соотнести их с международными стандартами информационной безопасности;

[1] Собрание законодательства Российской Федерации, 2002, 52, ст. 5140

[2] Собрание законодательства Российской Федерации, 2006, 31 (часть 1), ст. 3448

3.Обобщить международный опыт правоприменительной практики в сфере информационной безопасности на основе применения международных стандартов информационной безопасности;

4. Исследовать особенности информационных отношений в сети Интернет, как инфраструктуры глобального информационного общества и перспективных международных отношений, а также особенности сетевых информационных угроз;

5. Провести сравнительно - правовой анализ обеспечения информационной безопасности в сети Интернет;

6.Разработать рекомендации по развитию договорного режима оказания безопасных Интернет-услуг в России;

7.Разработать типовые нормативные акты Службы информационной безопасности кредитной организации;

8.Разработать рекомендации по нормативному обеспечению аудита информационной безопасности кредитной организации с учетом международного опыта;

9.Исследовать проблемы латентности и прогнозирования угроз информационной безопасности.

Объектом исследования являются информационные отношения, возникающие в связи с обеспечением безопасности национальных интересов в глобальной информационной сфере.

Предметом исследования являются международные нормы и стандарты регулирования информационной безопасности в информационных отношениях.

Степень разработанности темы исследования. Опубликованные и проводимые в информационно-правовом поле научные исследования охватывают широкий круг проблем. Так, изучались вопросы, касающиеся защиты авторских прав на произведения, доступные в сети Интернет, прав на доменное наименование, распространения вредной информации, оказания услуг посредством сети Интернет, ответственности за правонарушения в информационной среде Интернет, а также вопросы электронного документооборота, осуществления безналичных платежей с использованием телекоммуникационных сетей, заключения сделок в электронной форме с использованием электронной подписи и др.

Однако системное исследование международного опыта правого регулирования информационной безопасности и его применения в Российской Федерации с учетом роли информационных операций как источника крупномасштабных массированных угроз информационной безопасности до последнего времени не проводилось, равно, как недостаточно полно рассматривались в правовых исследованиях проблемы применения международных стандартов информационной безопасности. Не были ранее исследованы проблемы латентности и прогнозирования угроз информационной безопасности.

Методологическую основу исследования составляют такие научные методы, как анализ и синтез, индуктивный и дедуктивный методы, аналогия и моделирование, диалектическая логика и системный подход. В работе применялись и специальные методы: формально-юридический, сравнительно-правового исследования.

Нормативно-правовую основу исследования составляют российские и зарубежные правовые акты, действующие в области правового обеспечения информационной безопасности. Развитие и совершенствование законодательства в области правового регулирования информационной безопасности предусмотрено принятыми в Российской Федерации концептуальными и доктринальными документами. Среди них необходимо выделить Доктрину информационной безопасности Российской Федерации[3], одобренную Президентом Российской Федерации 9 сентября 2000 года, Концепцию национальной безопасности Российской Федерации в редакции, утвержденной Указом Президента Российской Федерации от 10 января 2000 года № 24[4], Концепцию внешней политики Российской Федерации, утвержденную Президентом Российской Федерации 28 августа 2000 года, Концепцию использования информационных технологий в деятельности федеральных органов государственной власти до 2010 года, одобренную распоряжением Правительства РФ от 27.09.2004г. № 1244-р.

Международную правовую основу регулирования общественных отношений в сфере информационной безопасности составляет достаточно большое количество директив, конвенций, деклараций, хартий. резолюций, рекомендаций, иных международных актов. Среди них необходимо выделить такие, как Резолюция 54/49 Генеральной Ассамблеи ООН «Достижения в сфере информатизации и телекоммуникации в контексте международной безопасности», принятая 1 декабря 1999 года на 54-й сессии Генеральной Ассамблеи ООН; Конвенция Совета Европы о киберпреступности от 23.11.2001г.; Конвенция ООН об использовании электронных сообщений в международных договорах 2005г.; Декларация «О европейской политике в области новых информационных технологий» 1999г.[5]; Декларация принципов построения информационного общества, принятая на Всемирной встрече на высшем уровне в Женеве в декабре 2003г.; Рамочное решение Европейского Союза об атаках на информационные системы от 24.02.2005г.; Рекомендации Совета Европы по защите неприкосновенности частной жизни в Интернете от 23.02.1999г.;

[3] Российская газета, 28.09.2000, 187, ст. 4

[4] Российская газета, 10.02.2000, № 2, ст. 170

[5] Совет Европы и Россия. Сборник документов /Отв. ред. Ю.Ю. Берестнев. – М.: Юрид. лит., 2004. – 928 с. – С. 860

Рекомендации Совета Европы № Rec (2001) 3 по предоставлению судами и оказанию других правовых услуг гражданам с помощью новых технологий от 28.02.2001г.; Рекомендации Совета Европы № 1706 «Средства массовой информации и терроризм» 2005г; Тунисское обязательство, принятое на Всемирной встрече на высшем уровне по вопросам информационного общества в 2005г. и др.

Теоретической основой исследования послужили труды ведущих ученых в области теории государства и права, философии права и в области информационного права, таких, как А.Б. Агапов, С.С. Алексеев, Ю.М. Батурин, И.Л. Бачило, А.Б. Венгеров, В.А. Копылов, В.Н.Лопатин, Е.А.Лукашева, Б.Н.Мирошников, Н.Н.Моисеев, А.В.Морозов, В.Б.Наумов, Т.АПолякова, Ю.Г.Просвирнин, М.М.Рассолов, А.Г.Серго, Ю.Ю.Соковых, А.А.Стрельцов, В.М. Сырых, Ю.А. Тихомиров, Б.Н. Топорнин, А.А. Фатьянов, Л.В.Филатова, А. В. Шамраев и др.

Использовались также труды таких зарубежных авторов, как Ю. Хаяши, И. Масуде, Т. Стоуньер, З. Бжезинский, Д. Белл, О. Тоффлер, Г. Кан и др.

Эмпирической основой исследования являются результаты, полученные автором в процессе работы начальником отдела защиты информации АСУ ВС РФ, в Межведомственном координационном совете по проблемам защиты информации ВПК, в финансовой корпорации «УРАЛСИБ», в диссертационных советах ВАГШ и МИФИ, в Российском фонде фундаментальных исследований и Федеральном агентстве по науке и инновациям по проблемам информационной безопасности; профессором кафедр компьютерного права, информационного права, уголовного процесса, геополитики; в Научном центре информационной безопасности Военной академии Генштаба ВС РФ, Академии военных наук по отделению национальной безопасности (секция информационной безопасности).

Научная новизна исследования состоит в том, что автором впервые проведено системное исследование международного опыта правового регулирования информационной безопасности и проблем его применения в кредитных организациях Российской Федерации с учетом особенностей национальных интересов и тенденций мирового развития.

В ходе исследования получены новые научные результаты:

1. Развита и конкретизирована теория правового обеспечения информационной безопасности А.А.Стрельцова. В частности, ключевые понятия этой теории дополнены по открытым источникам Словарем терминов и определений в области информационной безопасности[6],первичную подготовку которого осуществил автор, а также

[6]Словарь терминов и определений в области информационной безопасности. Научный центр информационной безопасности Военной академии Генерального штаба Вооруженных Сил Российской Федерации. М.: ВАГШ, 2004

каталогом зарубежных аббревиатур и глоссарием зарубежных терминов в области информационного противоборства. Классификация источников угроз информационной безопасности дополнена информационными операциями, осуществление которых регламентировано такими нормативными правовыми актами, как новый полевой устав Сухопутных войск, по вопросам ведения войсками информационной борьбы – FM-106 *«Информационные операции», «Объединенная доктрина информационных операций»* Комитета Начальников Штабов (США), инструкция КНШ *«О политике в совместных информационных операциях» и «О проведении оборонительных информационных операций»*, новый устав Сухопутных войск FM-1 «Операции», с объемным разделом *«Информационное превосходство»* и ряд других.

2.Разработаны предложения в раздел 1.2.5. *«Проблемы международно-правового регулирования в области информационной безопасности»* Основных направлений нормативного правового обеспечения информационной безопасности Российской Федерации, одобренных Межведомственной комиссией Совета Безопасности Российской Федерации по информационной безопасности 27 ноября 2001г. №4.1. Систематизированы международные нормы правового регулирования информационной безопасности, отмечена неполнота системы таких норм. Показана роль международных стандартов информационной безопасности в ее практическом обеспечении и роль международного гуманитарного права в информационной сфере при вооруженных конфликтах.

3.Обобщен международный опыт регулирования информационной безопасности. Показано, что практическое регулирование общественных отношений в области использования инфраструктуры информационного общества развивается в направлении повсеместного применения международных стандартов информационной безопасности, таких как ISO 17799. COBIT, BS 7799-2, ISO 9001 и др.

4. Разработана классификация информационных отношений в глобальной сети Интернет по признакам субъектного состава и по признакам информационного процесса, посредством которого удовлетворяются информационные интересы в информационных отношениях. Выявлено, что в сети Интернет может реализоваться 27 видов информационных отношений, из которых 9 видов содержат угрозы

5.Установлено, что законодательные инициативы правительств государств Европы, Азии и Америки свидетельствуют об отсутствии единого подхода по основополагающим принципам правового регулирования информационных отношений субъектов сети Интернет, их правам и обязанностям, пределам правового регулирования

информационных отношений субъектов, правовым механизмам защиты субъектов от угроз ИБ. Выделено два подхода к регулированию информационных отношений субъектов Интернет - европейский и азиатский. Сделан вывод, что в России подход к регулированию отношений абонента, оператора Интернет и третьих лиц не сформирован, но более соответствуют европейскому подходу.

6.На основании сравнительно-правого исследования для обеспечения информационной безопасности абонента сети Интернет выработаны рекомендации по разграничению прав, обязанностей и ответственности российского оператора Интернет и абонента в договорном режиме.

7.Установлено, что при разработке Концепции и политики информационной безопасности, положений о структурных подразделениях службы информационной безопасности, должностных инструкций ее сотрудников, других актов, в интересах интеграции России в мировое сообщество, в том числе посредством глобальной сети Интернет, необходимо выполнять требования международного стандарта информационной безопасности ISO 17799. Автор впервые в ОАО КБ «НИКойл», ФК «УРАЛСИБ» и в структурных подразделениях этих организаций лично реализовал требования этого стандарта при разработке перечисленных актов.

8. Выявлено, что нормативной основой проведения аудита информационной безопасности в развитых странах и в крупных корпорациях являются в основном стандарты Контроля COBIT и стандарт ISO 17799, которые использовались и автором при проведении аудита информационной безопасности с дополнением их в конкретных случаях профилями защиты.

9.Показано, что проблемы латентности и прогнозирования угроз информационной безопасности относятся к фундаментальным проблемам не только в области правового обеспечения информационной безопасности, но и в правовой науке в целом, так как их решение позволит управлять развитием правотворчества и правоприменения в широком диапазоне конфликтных ситуаций. На примере заведомо ложного сообщения об акте терроризма (ст.207 УК РФ[7]) показана методика решения этих проблем.

Положения, выносимые на защиту:

1. На основе анализа международных актов и законодательства Российской Федерации в понятийный аппарат, применяемый в правовом обеспечении информационной безопасности, в научно-практических целях вводятся термины и понятия современных информационных операций,

[7] Собрание законодательства Российской Федерации – 1996. - № 25. – С. 2954

как источника крупномасштабных массированных угроз информационной безопасности.

2.В систему правового регулирования в сфере информационного законодательства должны входить не только нормы международного права в информационной сфере, но и механизмы их реализации в виде международных стандартов информационной безопасности.

3.Практическое регулирование общественных отношений в области использования инфраструктуры информационного общества осуществляется в развитых странах в направлении применения международных стандартов информационной безопасности, таких как ISO17799, COBIT, BS 7799-2 и др.

4.Информационные отношения в глобальной сети Интернет классифицированы автором по признакам субъектного состава и по признакам информационного процесса, посредством которого удовлетворяются информационные интересы в информационных отношениях. Из 27 видов информационных отношений, которые теоретически могут реализовываться в сети Интернет, 9 содержат угрозы.

5.Сравнительно–правовое исследование выявило два подхода к регулированию информационных отношений оператора Интернет, абонента и других лиц (государственных органов). Первый подход – европейский, отличающийся демократичными принципами и свободой пользования сетью Интернет. Второй подход – азиатский, отличающийся стремлением установить полный контроль информационных потоков в национальном сегменте сети Интернет. В России подход к регулированию отношений абонента, оператора Интернет и третьих лиц не сформирован, но наметившиеся тенденции более соответствуют европейскому подходу.

6.На основании выводов сравнительно-правого исследования для обеспечения информационной безопасности абонента в России разработан механизм его правовой защиты, включающий полный перечень прав, обязанностей и ответственности субъектов сети Интернет.

7.При разработке Концепции и политики информационной безопасности, положений о структурных подразделениях службы информационной безопасности, должностных инструкций ее сотрудников, других юридически значимых актов, в интересах интеграции России в мировое сообщество, в том числе посредством глобальной сети Интернет, необходимо учитывать требования международного стандарта информационной безопасности ISO 17799.

8.Нормативной основой проведения аудита информационной безопасности в развитых странах и в крупных корпорациях являются стандарт контроля COBIT и стандарт ISO 17799. Эти стандарты должны использоваться и в России при проведении аудита информационной безопасности с дополнением их при необходимости профилями защиты.

9. В работе на примере заведомо ложного сообщения об акте терроризма (ст.207 УК РФ), которое является видом информационной угрозы, показано возможное решение проблем латентности и прогнозирования угроз ИБ на основе методов правовой статистики и регрессионного анализа. Полученные результаты верифицируются прогнозами и последующими статистическими наблюдениями.

Теоретическая значимость Изучение международного опыта правового регулирования информационной безопасности и его применение в Российской Федерации является актуальным для развития законодательства. Методика исследования проблем латентности и прогнозирования заведомо ложных сообщений об актах терроризма имеет общетеоретическую значимость, поскольку может применяться при решении других проблем правовой науки и смежных с ней областей знаний, например, при исследовании аналогичных проблем по другим составам уголовных преступлений и административных правонарушений.

Практическая полезность работы заключается в том, что выводы и предложения, содержащиеся в диссертации, реализуются в НИОКР народнохозяйственного и оборонного значения, используются в учебном процессе РПА Минюста России, МИФИ, ВАГШ, ВУ Минобороны России, НИЕВ при разработке учебных курсов и программ, проведении занятий по проблемам информационного права и сети Интернет со студентами юридических вузов, слушателями высших военных учебных заведений и военными юристами, а также на курсах повышения квалификации федеральных судей, при подготовке аспирантов и адъюнктов, при разработке и правовом сопровождении веб-сайта Академического правового колледжа РПА Минюста России, при оформлении уголовных и гражданских дел в гипертекстовом и гипермедийном виде, в производственной деятельности ФК «УРАЛСИБ», ОАО «РОСБАНК» и др.

Апробация результатов исследования. Основные результаты работы докладывались и обсуждались на заседаниях кафедр и межвузовских семинарах, на международных, всесоюзных и всероссийских научно-практических конференциях по проблемам информационной безопасности, на ежегодных Международных Екатерининских чтениях и Международных Державинских чтениях и опубликованы в 50 из 200 научных работах

Структура диссертации состоит из введения, трех глав, каждая из которых содержит три параграфа с обоснованием в них соответствующих новых научных положений, заключения, списка литературы и десяти приложений, содержащих детальные обоснования результатов работы, которые в основной текст диссертационного исследования не включены ввиду значительного объема.

СОДЕРЖАНИЕ ДИССЕРТАЦИИ

Во **введении** обосновывается актуальность темы, степень ее разработанности, определяются цель, объект, предмет и задачи исследования, характеризуется теоретическая и методологическая основа работы, обосновываются научная новизна и значимость для теории и практики предпринятого исследования, формулируются основные положения, выносимые на защиту.

Глава 1.«Международный опыт правового регулирования информационной безопасности» является теоретической частью диссертации

В параграфа ***1.1. «Информационная безопасность: понятийный аппарат, источники угроз, роль информационных операций»*** автором в интересах системного и согласованного характера проводимых исследований в составе группы ведущих специалистов была подготовлена первая редакция словаря терминов и определений в области информационной безопасности, как отправная точка доказывания результатов исследования, которая затем обсуждалась и дополнялась.

В Словарь вошли термины, отобранные на основе систематизации, обработки, обобщения и дополнения материалов, подготовленных Управлением информационной безопасности Аппарата Совета Безопасности РФ, Главным оперативным управлением Генерального штаба ВС РФ, Центром военно-стратегических исследований Генерального штаба ВС РФ, Государственной технической комиссией при Президенте РФ, Федеральным агентством правительственной связи и информации при Президенте РФ, Федеральной службой безопасности РФ, Службой внешней разведки РФ, Министерством внутренних дел РФ, Министерством юстиции РФ, а также термины действующих нормативных и руководящих документов, государственных и отраслевых стандартов Российской Федерации и открытых публикаций в отечественной печати. Словарь предназначен для специалистов, занимающихся вопросами информационной безопасности и рекомендован для использования в деятельности органов государственного и военного управления при обеспечении мероприятий информационной безопасности, а также при проведении исследований и в учебном процессе. Словарь разработан в Научном центре информационной безопасности Военной академии Генштаба ВС РФ авторским коллективом в составе: ГРИНЯЕВА С.Н., КОМОВА С.А., КОРОТКОВА С.В. КРЫЛОВА Г.О.,КУЗНЕЦОВА Ю.В., МЕЛЕШИНА В.Я, ОСТАНКОВА В.И., ПАЛИЯ А.Ф., РОДИОНОВА С.Н.

Кроме того, автором был осуществлена систематизация зарубежной терминологии и аббревиатур с использованием официальных веб–

сайтов[8] авторитетных органов и организаций США, таких как Белый дом, Центр защиты национальной инфраструктуры, Управление защиты критической инфраструктуры, Министерство национальной безопасности, Центральное разведывательное управление, Пентагон, Комитет начальников штабов, Сайт объединенных доктрин Комитета начальников штабов, Электронная библиотека Комитета Начальников Штабов, Агентство перспективных исследований министерства обороны США, Центр информационной борьбы ВВС, Агентство информационных систем министерства обороны США, Программа совместных исследований систем связи, компьютерных систем, разведки и наблюдения, Федеральная комиссия по коммуникациям, Национальный университет обороны, Сайт Федерации американских ученых, Гудзоновский Институт стратегических исследований имени Германа Кана, Корпорация РЭНД, Национальный научный фонд, Координационный центр групп чрезвычайного реагирования на компьютерные инциденты, Глобальная система управления войсками, Бюро международных информационных программ и др.

Далее на основе систематизированного понятийного аппарата, теоретических и методологических основ правового обеспечения информационной безопасности России, разработанных А.А.

---

[8] Белый дом *(White House)*- http://www.whitehouse.gov/; Центр защиты национальной инфраструктуры *(National Infrastructure Protection Center)*- http://www.nipc.gov/; Управление защиты критической инфраструктуры *(Critical Infrastructure Assurance Office (CIAO))*- http://www.ciao.gov/; Министерство национальной безопасности (*Department of Homeland Security)*- http://www.dhs.gov; Центральное разведывательное управление *(Central Intelligence Agency)*- http://www.odci.gov/; Пентагон *(The Pentagon)*- http://www.defenselink.mil/pubs/pentagon/; Комитет начальников штабов *(Joint Chiefs Page)*- http://www.dtic.mil/jcs; Сайт объединенных доктрин Комитета начальников штабов *(Joint Doctrine)*- http://www.dtic.mil/doctrine/; Электронная библиотека КНШ *(Joint Electronic Library)*- http://www.dtic.mil/doctrine/jel/index.html; Агентство перспективных исследований министерства обороны США *(Defense Advanced Projects Research Agency (DARPA))*- http://www.darpa.mil; Центр информационной борьбы ВВС *(Air Force Information Warfare Center (AFIWC))*- http://www.aia.af.mil/aialink/homepages/afiwc/index.htm; Агентство информационных систем министерства обороны США *(Defense Information Systems Agency)*- http://www.disa.mil/; Программа совместных исследований систем связи, компьютерных систем, разведки и наблюдения *(The C4ISR Cooperative Research Program (CCRP))*- http://www.dodccrp.org/ ; Федеральная комиссия по коммуникациям *(Federal Communications Commission (FCC))* -http://www.fcc.gov; Национальный университет обороны *(National Defense University)*- http://www.ndu.edu/; Сайт Федерации американских ученых *(Federation of American Scientist's)*- http:/www.fas.org/; Институт стратегических исследований *(Institute for National Strategic Studies)* - http://www.ndu.edu/inss/insshp.html; Корпорация РЭНД *(RAND National Defense Research Institute)*- http://www.rand.org/; Национальный научный фонд *(The National Science Foundation)*- http://www.nsf.gov/; Координационный центр групп чрезвычайного реагирования на компьютерные инциденты *(CERT Coordination Center)* - http://www.cert.org/; Глобальная система управления войсками *(Global Command and Control System)*- http://gccs.disa.mil/gccs/index.html; Бюро международных информационных программ- http://usinfo.state.gov/.

Стрельцовым[9], кратко изложена авторская версия теории правового регулирования информационной безопасности по состоянию на 2007 год. Этот фрагмент работы введен для придания ей системности и целостности. Используются общепринятые термины и определения, такие как информация, информационные ресурсы, информационная инфраструктура, информационная сфера, национальные интересы в информационной сфере, информационная безопасность, угрозы информационной безопасности, источники угроз информационной безопасности и др. На основе исследования открытых документальных источников США предложено использовать понятие информационных операций как источника крупномасштабных массированных угроз информационной безопасности.[10]

В параграфе *1.2.* ***«Международные нормы регулирования информационной безопасности»*** проведена систематизация международных норм регулирования информационной безопасности. Среди методов обеспечения информационной безопасности системообразующими являются методы нормативного правового регулирования общественных отношений в информационной сфере. При этом в силу глобализации информационного общества весьма существенным является международно-правовой режим информационной безопасности. Такой режим создается нормами международного права, в том числе нормами *международного гуманитарного права,* которое устанавливает правила ведения военных конфликтов, включая нормы регулирования отношений *в информационной сфере*. Эти нормы в равной степени должны распространяться и на *информационные войны* (операции). Концепция международного гуманитарного права основана на триаде *« гуманность - боевая необходимость - соразмерность».* Важнейшими международными актами новейшей истории являются Окинавская хартия глобального информационного общества, Декларация о европейской политике в области новых информационных технологий, Декларация Комитета Министров Совета Европы о правах человека и верховенстве права в информационном обществе и др. Каждый из таких и аналогичных актов предусматривает меры по обеспечению информационной безопасности. Рекомендуется поощрять установление международных *стандартов* и гарантий, необходимых для обеспечения подлинности передаваемых электронными средствами документов и сообщений, имеющих обязательную юридическую силу. Наряду с этим принят также ряд нормативных актов в области *стандартизации*. К их

[9] Стрельцов А.А.Теоретические и методологические основы правового обеспечения информационной безопасности России: Автореф. дис. ... д-ра юрид. наук: 05.13.19 / Московский инженерно – физический институт. М., 2004.

[10] Дербин Е.А., Крылов Г.О.и др. Информационные операции современности. Учебное пособие/ Военная академия Генерального штаба ВС РФ, М., 2004

числу можно отнести такие, как Устав международного союза электросвязи от 22.12.1999; Рекомендации Европейской экономической комиссии ООН относительно политики в области стандартизации (1996); Рекомендация № 25 Европейской экономической комиссии ООН «Использование стандарта Организации Объединенных Наций для электронного обмена данными в управлении, торговле и на транспорте» от 09.1996; Рекомендация № 26 Европейской экономической комиссии ООН «Коммерческое использование соглашений об обмене для электронного обмена данными» от 03.1995; Директива Совета Европейского Сообщества № 89/336 «О согласовании законодательных актов государств-участников Сообщества, касающихся электромагнитной совместимости» от 03.05.1989; Рекомендация № R (2003) 15 Комитета министров Совета Европы «Об архивации электронных документов в правовой сфере» от 09.09.2003 и др.

Среди нормативных правовых актов государств-участников СНГ необходимо отметить Решение Совета глав правительств СНГ «О концепции информационной безопасности государств-участников Содружества Независимых Государств в военной сфере» от 04.06.1999; Соглашение о сотрудничестве в формировании информационных ресурсов и систем, реализации межгосударственных программ государств - участников Содружества Независимых Государств в сфере информатизации» от 24.12.1999; Соглашение об основах гармонизации технических регламентов государств-членов Евразийского экономического сообщества от 24.03.2005 и др.

В параграфе ***1.3. «Международный опыт нормативного регулирования информационной безопасности»*** кратко рассмотрена эволюция противодействия компьютерным преступлениям, которые получили широкое распространением с началом массового освоения персональных компьютеров, а затем и сетевых технологий. На международном уровне первая попытка комплексного рассмотрения проблем компьютерной безопасности в уголовном праве была предпринята Организацией экономического сотрудничества и развития (ОЭСР) в 1986 году, затем аналогичные попытки предпринимались в 1989г. Комитетом Министров стран-членов Совета Европы, в 1996г. был принят Модельный уголовный кодекс для стран-участниц СНГ, а 23.11.2001г была принята Конвенция Совета Европы о киберпреступности, которая упорядочила составы компьютерных преступлений. Однако, трансграничный характер таких преступлений, трудности их локализации и доказывания в судах стимулировали развитие практики комплексного обеспечения информационной безопасности на основе ведомственных, отраслевых, национальных и международных стандартов, которые стали динамично разрабатываться и повсеместно использоваться. Это привело к созданию Международной

Электротехнической Комиссии (IEC), а затем и Международной Организация по Стандартизации (ISO)[11]. Стандарты часто еще называют лучшими практиками. Их количество увеличивается в связи с растущим многообразием обстоятельств, в которых они применяются как стандарты *de* facto, Стандарты образуют иерархическую систему. По состоянию на апрель 2007г. такая система насчитывает несколько десятков стандартов, применение которых комплексно обеспечивает безопасность и качество функционирования человеко-машинных систем на всех этапах их жизненного цикла. Высокоуровенные стандарты часто называют процессными, процедурными или тактическими, т.к. они описывают процессы, процедуры. К их числу относятся такие, как:

- Управление информационными системами - COBIT, BS 15000[12], Microsoft Operations Framework и ITIL;
- Управление проектами - PRINCE2 и the PMBOK;
- Управление безопасностью - ISO 13335, ISO 13569 (банковские и финансовые услуги), ISO 17799/BS 7799-2 (оба локализованы для многих стран), IT Baseline Protection Manual (Германия), ACSI-33[13](Австралия), множество стандартов National Institute of Standards and Technology[14] - *NIST Handbook* (SP800-12, USA), CobiT® *Security Baseline*™, ENV12924 (Медицинская информатика) и the Information Security Forum *Standard of Good Practice*[15]*;*
- Управление качеством—ISO 9001, EFQM и Baldrige National Q- Plan;
- Программирование—TickIT, Capability Maturity Model Integration (Software Engineering Institute);
- IT Governance - COBIT, *IT Governance Implementation Guide*, COSO *Internal Control - Integrated Framework* и COSO *Enterprise Risk Management - Integrated Framework*, и недавно разработанный Австралийский стандарт AS 8015-2005 (корпоративное управление информационными и коммуникационными технологиями);
- Управление рисками - Австралийский стандарт AS/NZS 4360[16];
- BCP (планирование непрерывности бизнеса) - British Standards Institution PAS-56 и Австралийский стандарт HB 221-2004;
- Аудит ИС - COBIT и ISO 19011;

[11] www.iso.ch
[12] www.bsi-global.com.
[13] Australian Communications-Electronic Security Instruction 33, www.dsd.gov.au/infosec/publications/acsi33.html
[14] www.nist.gov
[15] www.isfsecuritystandard.com
[16] Standards Australia, www.standards.com.au

Наибольшее и универсальное распространение из процессных стандартов получили стандарты ISO 17799, COBIT, ISO 9001, BS 7799-2 и их сочетания.

Кроме большого числа процессных стандартов, имеется еще большее число эксплуатационных, технических стандартов. Международная Организация по Стандартизации (ISO), Европейский Институт Стандартов Телекоммуникаций и Национальный Институт Стандартов и Технологии (NIST) издали стандарты по таким вопросам, как шифрование (FIPS 197), критерии (технические) оценки безопасности ИТ (ISO 15408), планирование непрерывности бизнеса (FIPS 87), использование паролей (FIPS 112) и др. Стандарты информационной безопасности, качества и управления в обязательном порядке учитываются при проведении сертификации и аудита. Использование стандартов увеличивает ценность продуктов, создаваемую информационными технологиями, но нет таких стандартов, которые охватывали бы все аспекты управления информационной безопасностью. Состояние вопроса в этой области аналогично состоянию вопроса в системном анализе, ибо последний вырабатывает плохие решения по сложным проблемам, по которым другими методами вырабатываются еще худшие решения.

Глава 2. «Применение международного опыта регулирования информационной безопасности в глобальной сети Интернет» в равной мере относится как к международной, так и к российской проблематике нормативного регулирования информационной безопасности, т.е. играет связующую роль между теоретической и практической (реализационной) частями диссертационного исследования.

В параграфе ***2.1. «Международная практика информационных отношений и угрозы в глобальной сети Интернет»*** исследуются основные элементы и угрозы информационных отношений в глобальной сети Интернет. К основным элементам информационного правоотношения относятся: субъекты, вступающие в правоотношения при осуществлении информационных процессов; объекты, в связи с которыми субъекты вступают в информационные правоотношения, содержание прав и обязанностей субъектов по осуществлению действий над объектами информационного правоотношения, ответственность субъектов при нарушении прав или невыполнении обязанностей по отношению к другим субъектам правоотношения. Субъектами информационных правоотношений являются оператор Интернет-связи, его абонент, другие пользователи Интернет, правоохранительные органы. Содержание прав и обязанностей перечисленных субъектов взаимосвязано с их возможностями совершать определенные действия с объектами информационных правоотношений, в том числе и причиняющие вред. Объектами в информационных отношениях абонента и оператора Интернет-связи являются информация, информационные продукты и

услуги, состояние защищенности личности, защищенность информации. Действия субъектов таких отношений, способных повлиять на информационную безопасность личности, являются основанием их ответственности. К возможным действиям абонента относятся: просмотр веб-страниц, получение и отправка электронных сообщений, хостинг. К возможным действиям оператора Интернет-связи относятся сбор сведений об информационном обмена абонента, воздействие на информационный обмен абонента путем изменения скорости обмена, фильтрации содержимого передаваемой информации, воздействия на информацию опубликованную пользователем на веб-странице, размещенной на сервере оператора, сбор персональных данных о пользователе. Возможные действия правоохранительных органов заключаются в истребовании от оператора Интернет-связи или его абонента необходимой им информации об информационном обмене абонента. К действиям других пользователей Интернета, имеющих значение для информационной безопасности абонента, можно отнести только намеренные действия по получению несанкционированному доступу к его информации на веб-странице, в компьютере, в электронном письме. Просмотр веб-страниц несет в себе две угрозы. Это вредная информация, размещенная непосредственно на странице (фото, видео, аудио, текстовые данные), и вредоносные программные коды, запускаемые с различными приложениями, которые обслуживают правильное отображение просматриваемой страницы, способные изменить состояние информации в компьютере пользователя. Вредная информация способна оказывать воздействие на пользователя при посещении веб-страниц, на которых она расположена. Попадание вредной информации на экран монитора пользователя зависит, в основном, от действий самого пользователя, так как он сам осуществляет передвижение по сети Интернет, и решает, какая информация подлежит его вниманию.

Ограничение на доступ к вредной информации может быть установлено самим оператором Интернет-связи. Это возможно за счет применения им специальных программных фильтров, позволяющих перекрывать доступ к информации определённого содержания, в том числе и не относящейся к вредной. Большинство операторов Интернет-связи имеют программные фильтры и могут применять их по договорённости с абонентом. Другим видом действий абонента является получение электронных сообщений. В этом случае существуют угрозы воздействия вредной информации, размещенной в электронном сообщении, получение и заражение компьютерными вирусами, получение не запрашиваемой информации (*спам*). В действиях пользователя по отправке электронных писем существуют такие угрозы, как недоставка отправленного письма до адресата и нарушение конфиденциальности информации, содержащейся в письме. Данные угрозы могут быть реализованы как в результате действий самого пользователя, так и в

результате действий или бездействия оператора Интернет-связи. Так при отсутствии соединения или при некачественном соединении с сетью Интернет абонент не сможет отправить электронную корреспонденцию. Кроме того угроза недоставки электронного письма или нарушения его конфиденциальности может быть реализована в результате неправильной работы почтовых серверов оператора Интернет-связи, в результате использования фильтров на исходящую от абонента информацию, в силу форс-мажорных обстоятельств. Нарушение конфиденциальности электронной переписки абонента может быть в результате несанкционированного доступа третьих лиц к его компьютеру или электронному почтовому ящику. При опубликовании своей веб-страницы в сети Интернет для информационной безопасности пользователя существуют такие угрозы, как несанкционированный доступ к опубликованной информации и, следовательно, нарушение данных аутентификации абонента, изменение или удаление веб-страницы пользователя и ей блокировка, как результат несанкционированного доступа. Источником таких угроз может быть как оператор Интернет-связи, так и другие пользователи Интернет. В первом случае возможность несанкционированного доступа возможна в силу того, что оператор Интернет-связи является хранителем данных аутентификации (пароля и логина) пользователя при доступе к редактированию своей страницы. Во втором случае доступ к странице абонента может быть осуществлен в силу получения другими пользователями Интернет данных аутентификации, необходимыми для управления страницей. Данная информация может быть получена в результате её хищения путем несанкционированного доступа к файлам (взлома) оператора Интернет-связи или любым другим способом. Еще существуют угрозы, возникновение которых не зависит от деятельности абонента в глобальной сети. К ним относятся диффамация, нарушение авторских прав, распространение персональных данных.

В параграфе ***2.2 «Сравнительно-правовой анализ обеспечения информационной безопасности в сети Интернет»*** рассмотрены нормы права, определяющие позицию стран Европейского Содружества, Соединенных Штатов Америки и Канады. Так, в законе США «Об авторском праве в цифровую эпоху» 1998г. (Digital Millennium Copyright Act) устанавливается ограниченная ответственность оператора Интернет-связи, запрещающая в определённых случаях нарушения авторских прав применять к ним санкции. Подобным образом обстоят дела и с информацией клеветнического характера. В 1996 году Конгресс США одобрил норму, фактически исключающую возможность возбуждать дела о клевете в Интернете против операторов Интернет-связи. Похожая схема регулирования используется Европейским сообществом. Важным комплектом нормативных документов, оказывающих решающее влияние на правовые нормы европейских стран в области Интернета, являются

нормативные документы Европарламента и Совета Европы. К ним относятся такие документы, как Декларация свободы общения в Интернете, директива 97/66/ЕС «Об обработке персональных данных и защите частных интересов в области телекоммуникации», Директива 2000/31/ЕС 2000г. «Об электронной коммерции», Конвенция Совета Европы по киберпреступности от 2001г. Эти и другие документы составляют основу европейской нормативной базы в области Интернета. Так, в Декларации свободы общения в Интернете определены основные принципы, призванные гарантировать соблюдение прав человека при пользовании глобальной компьютерной сетью. Рассмотрены также нормативные акты, характеризующие политику правового регулирования деятельности операторов Интернет-связи, осуществляемую в странах восточной части земного шара (Китай, Япония, Сингапур, Таиланд, Корея и др.). Наиболее четкий подход правового регулирования указанной деятельности сформирован Китаем. Основными документами, регулирующими китайский сегмент Интернета, являются такие акты Госсовета КНР, как «Правила защиты безопасности компьютерных систем» (действуют с 1994г.), «Временное положением о контроле над международными соединениями информационных компьютерных сетей» (с 1996г.), «Временное положением о контроле над электронными изданиями» (с 1996г.), «Правила защиты безопасности международных соединений информационных компьютерных сетей» (с 1997г.). После образования Сетевого информационного центра Китая (CNNIC) были опубликованы «Временный порядок регистрации названий Интернет-страниц» и «Правила контроля за помещением информации в сети». Основные особенности Китайской Интернет-политики, в области защиты публичных и частных интересов – это стремление к полному контролю над процессами использования глобальной сети.

В параграфе ***2.3. «Инициативы по развитию договорного режима оказания безопасных Интернет-услуг в России»*** обоснована и приведена примерная редакция нормативных положений, которые необходимо включать в договор оказания услуг Интернет-связи, заключаемый между оператором Интернет-связи и абонентом, для обеспечения информационной безопасности абонента. Оператор Интернет-связи должен: предоставлять доступ к сети Интернет надлежащего качества в период всего времени указанного в договоре; по заявлению абонента применять специальные программы-фильтры для предотвращения посещения абонентом веб-страниц, содержащих информацию, направленную на разжигание ненависти, вражды и насилия, и непристойную информацию; по заявлению абонента использовать имеющиеся у него программные фильтры для предотвращения попадания в электронный ящик абонента информации незапрашиваемой абонентом (спам), а также компьютерных вирусов, содержащихся в электронных

письмах. При возникновении случаев удаления электронного письма, адресованного абоненту и содержащего важную для абонента информацию, оператор не несет ответственности за весь ущерб, прямо или косвенно причинённый абоненту, вследствие таких инцидентов. Оператор Интернет-связи не несёт ответственность за возникновение случаев проникновения компьютерных вирусов в компьютер абонента при получении электронных писем. Оператор Интернет-связи не несет ответственность за недоставку электронных писем абонента вследствие неправильного использования последним программ информационного обмена. Оператор Интернет-связи не несет ответственность за недоставку электронных писем и иной информации абонента, в случае отказа технического оборудования оператора по причинам от него не зависящим, к числу которых, относятся: природные техногенные катастрофы, иные аварийные ситуации, возникающие не по вине оператора, умышленное повреждение оборудования оператора третьими лицами, атаки злоумышленников с целью вывода из состояния нормального функционирования оборудования оператора, неработоспособности Интернет-узлов, обеспечивающих доставку письма абонента, расположенными за пределами зоны ответственности оператора, обстоятельств непреодолимой силы в общепринятом смысле. Оператор Интернет-связи в случае предъявления претензий от пострадавших лиц или получения требований правоохранительных органов имеет право проверить почтовые ящики абонента, ставшие источником проблем, и заблокировать их в случае необходимости. Оператор Интернет-связи не должен нести ответственность за содержание информационных ресурсов, создаваемых и поддерживаемых абонентом, и осуществлять какую-либо предварительную цензуру, однако в случае размещения абонентом на своих ресурсах информации, нарушающей права третьих лиц, а также информации, запрещенной законодательством, в частности, порнографических материалов, призывов к насилию, свержению власти и т.п., оператор оставляет за собой право заблокировать доступ к информационным ресурсам абонента. Оператор Интернет-связи не несет ответственность за изменение, удаление или блокирование информации на информационных ресурсах абонента, размещенных в сети Интернет, вследствие неправомерных действий третьих лиц. Оператор Интернет-связи не несёт ответственность за несанкционированный доступ третьих лиц к информации, находящейся в компьютере абонента. Абонент обязан использовать услуги Исполнителя следующим образом: не распространять запрещенную и не запрашиваемую информацию, не осуществлять несанкционированный доступ к закрытой информации, и не нарушать своими действиями информационные интересы третьих лиц. Абонент несет ответственность в случае использования сервисов обмена электронной почты для массовой рассылки информации,

незапрашиваемой другими пользователями Интернет (спам). Абонент несет ответственность в случае размещения в сети Интернет информации, нарушающей права и интересы других пользователей сети Интернет. Абонент несет ответственность в случае осуществления несанкционированного доступа к информации конфиденциального характера, принадлежащей оператору Интернет-связи или каким-либо пользователям сети Интернет. На основании изложенных правил составлена примерна редакция договоров об оказании услуг Интернет-связи, приведеная в приложениях к работе.

Глава 3. «Применение международного опыта правового регулирования информационной безопасности в Российской Федерации» является реализационной частью исследования.

Параграф ***3.1. «Применение международных стандартов в разработках нормативных корпоративных актов»*** обобщает 20-летний опыт нормотворчества автора в области защиты информации и информационной безопасности крупномасштабных систем. Именно примат правового обеспечения таких систем сместил научные интересы автора, в то время уже доктора физико-математических наук, профессора в область права. Договорная работа, разработка технических заданий, программ и методик испытаний, стандартов, положений, инструкций, других юридически значимых и практически необходимых актов регулирования производственных отношений, убедили автора в том, что в этой области, требующей согласованных действий большого числа лиц, много белых пятен. В советское время международные стандарты в закрытых учреждениях не применялись, применялись Единая Система Программной Документации (ЕСПД), многочисленные ГОСТы, ОСТы, СТП, ТЮ, другие технические и социотехнические нормы. Вместе с тем, будучи секретарем Генерального конструктора АСУ ВС академика Семенихина В.С. автор готовил по его поручению первые редакции правовых актов союзного уровня таких, как Проект Закона « Об информации, информатизации и защите информации», Положение о ГК ВТИ при СМ СССР, Положение о Межведомственном координационном совете по проблеме защиты информации в АСУ при КП СМ СССР по военно-промышленным вопросам и др. Международные стандарты информационной безопасности автор стал исследовать и применять практически с 1999 года при формировании Дирекции аудита и методологии информационной безопасности крупной многопрофильной финансовой корпорации. Автор лично разработал пакет новых нормативных актов на основе международного стандарта ISO 17799, который использовался также несколько позже при разработке концепций информационной безопасности ГАС «ПРАВОСУДИЕ» и Центрального Банка России. Пакет таких нормативных актов, разработанных автором, в

частности, включал в свой состав Концепцию информационной безопасности Финансовой корпорации «УРАЛСИБ», Политику информационной безопасности Финансовой корпорации «УРАЛСИБ», Положение о Дирекции аудита и методологии информационной безопасности Финансовой корпорации «УРАЛСИБ», должностные инструкции сотрудников Дирекции аудита и методологи информационной безопасности Финансовой корпорации «УРАЛСИБ» и др. Эти нормативные акты были разработаны на основе международного стандарта информационной безопасности ISO 17799 и его десяти ключевых областей в соответствии с общепринятой практикой. Полные тексты некоторых нормативно-правовых актов, разработанных автором с учетом международных стандартов, приведены в приложениях к работе.

Параграф ***3.2.«Нормативное обеспечение аудита информационной безопасности с учетом международного опыта».*** Темпы развития современных информационных технологий значительно опережают темпы разработки рекомендательной и нормативно-правовой базы руководящих документов, действующих на территории России. Поэтому вопрос аудита, «как оценить уровень безопасности корпоративной информационной системы», – обязательно влечет за собой следующие: в соответствии с какими критериями производить оценку эффективности защиты, как оценивать и переоценивать информационные риски предприятия? Вследствие этого, в дополнение к требованиям, рекомендациям и руководящим документам Государственной комиссии по техническому и экспортному контролю (ранее Гостехкомисии, далее по тексту Гостехкомиссии по тем подзаконным актам, которые были ею выпущены до Административной реформы) России приходится адаптировать к нашим условиям и применять методики международных стандартов (ISO 17799, 9001, 15408, BSI и пр.), а также использовать методы количественного анализа рисков в совокупности с оценками экономической эффективности инвестиций в обеспечение безопасности и защиты информации. В зарубежных нормативных документах установлен набор требований для различных типов средств и систем информационных технологий – в зависимости от различных условий их применения. Особенности развития отечественной нормативной базы в данной области заключаются в том, что отсутствует комплексный подход к проблеме защиты информации (рассматриваются в основном вопросы несанкционированного доступа к информации и вопросы обеспечения защиты от побочных электромагнитных излучений и наводок) и, кроме того, разработанные национальные стандарты и РД Гостехкомиссии России 1992-1996 не принимали во внимание международные стандарты ИСО/МЭК**.** На сегодняшний день эти недостатки начали устраняться. В целях совершенствования отечественной нормативной базы с 2001 года Гостехкомиссия и Госстандарт России совместно с другими

заинтересованными министерствами и ведомствами реализуют новые инициативы в этом направлении. В частности, утверждены три стандарта, определяющие критерии оценки безопасности информационных технологий. Они устанавливают требования к формированию заданий по оценке безопасности в соответствии с положениями международных стандартов. По линии Гостехкомиссии созданы несколько руководящих документов, в том числе «Руководство по разработке профилей защиты», «Руководство по регистрации профилей защиты», «Методология оценки безопасности информационных технологий» и «Автоматизированный комплекс разработки профилей защиты». Перечисленные документы по сути представляют собой прямую трансляцию положений международных стандартов ISO на российскую нормативно-техническую базу. В дополнение к ним создаются еще шесть спецификаций на защитные профили для операционных систем, межсетевых экранов, систем управления базами данных, автоматизированных систем учета и контроля ядерных материалов и др. Утвержден государственный стандарт РФ, определяющий процессы формирования средств проверки ЭЦП, идет работа по переводу данного стандарта в категорию межгосударственного. В 2000-2001 гг. была создана «Программа комплексной стандартизации в области защиты информации на 2001-2010 годы», в которой применён комплексный метод стандартизации. ПКС предусматривает появление примерно 40 ГОСТов. Кроме того, ВНИИ «Стандарт» разрабатывает проект «Программы комплексной стандартизации в области защиты информации, составляющей государственную тайну». В ее рамках планируется принятие 42 национальных стандартов и других нормативных документов. В свою очередь, Госстандарт разработал и представил на утверждение в Правительство РФ проект «Программы по разработке технических регламентов на 2003—2010 годы». В ходе ее выполнения создаются следующие документы: «Общий технический регламент безопасности информационных технологий», «Общий технический регламент требований к системам безопасности информационных технологий», «Общий технический регламент требований по защите информации, обрабатываемой на объектах информатизации» и «Специальный технический регламент требований по защите информации в оборонной промышленности». В 2003 году Госстандарт разработал проект классификатора техники и средств защиты информации, требований к контролю за эффективностью средств защиты информации и соответствующих систем управления. Создан проект государственного стандарта, включающего в себя общие положения по формированию системы управления качеством при разработке, изготовлении, внедрении и эксплуатации техники защиты информации. Внедрение этих нормативных документов обеспечит единую классификацию механизмов и техники

защиты информации, позволит определить основные характеристики систем качества техники защиты информации. Благодаря этому уменьшится разобщенность разработчиков и изготовителей, повысится уровень координации производителей специальной аппаратуры. Из анализа действующих нормативных документов по стандартизации в данной области следует, что по охвату регулирования аспектов безопасности ИТ, по детализации рассматриваемых в них проблем российские национальные стандарты всё ещё уступают международным. Вопросы стандартизации в сфере IT-безопасности решаются на международном уровне – совместным техническим комитетом СТК1 ИСО/МЭК «Информационные технологии», на региональном – европейскими организациями СЕН, ЕКМА и др., на национальном уровне – АНСИ, НИСТ (США), ДИН (Германия) и др. В некоторых из перечисленных работ принимал участие и автор, в основном как эксперт.

Параграф ***3.3. «Проблемы латентности[17] и прогнозирования угроз информационной безопасности»*** посвящен малоисследованным, но весьма актуальным проблемам правовой науки. Проблемы были поставлены и предложены автору для решения более десяти лет назад одним из ведущих криминологов С.М.Иншаковым. Их частное решение получено на примере таких информационных угроз, как заведомо ложные сообщения об актах терроризма, предусмотренные ст.207 УК РФ. Решение этой проблемы[18], полученное автором совместно Г.Л. Куликовой[19], было оценено криминологами как ***принципиально новое***. Актуальность проблем обусловлена тем, что, с одной стороны, по оценке В.В. Лунеева, латентная преступность ежегодно приближается к 80 % от реальной преступности (в европейских странах – к 50 %), с другой стороны, несмотря на комплекс предпринимаемых мер по предупреждению заведомо ложных сообщений об акте терроризма, рост количества этих преступлений в России продолжается, причем охватываются регионы, ранее не знавшие такого преступления. Так, если в 1997г. в России было зарегистрировано 1 386 преступлений, предусмотренных ст. 207 УК РФ, то в 2003г. – 7 811. Решение проблем было получено следующим образом. В результате применения методики, основу которой составил комплекс приемов статистического наблюдения,

[17] Латентная преступность в Российской Федерации за 2001-2002гг.(статистический сборник): Научно-практическое пособие/П.Э.Жигоцкий, Г.О.Крылов и др. –М.: РПА МЮ РФ, 2004

[18] Крылов Г.О., Куликова Г.Л. Криминологический анализ взаимосвязи актов терроризма и заведомо ложных сообщений о них: Методическое пособие.- М.: РПА МЮ РФ -2004.

[19] Куликова Г.Л. Заведомо ложное сообщение об акте терроризма: уголовно-правое и криминологическое исследование, Автореф. дис. ... канд. юрид. наук: 12.00.08 / Рос. правовая акад. М-ва юстиции РФ. М., 2004.

экспертная оценка материалов из прокуратур об отказе в возбуждении уголовных дел, выборочный анкетный опрос экспертов всех категорий, сотрудников правоохранительных органов (Генеральной прокуратуры РФ, МВД России, ФСБ России и др.), установлено, что латентная преступность заведомо ложных сообщений об акте терроризма в 2003г. составила 7 426 преступлений (зарегистрированная преступность – 7 811 преступлений), то есть фактическое количество преступлений достигает 15 237. Таким образом, коэффициент латентности составил 1,95.

Сложнее дело обстояло с прогнозом преступлений этого состава.

Главная задача исследования заключалась в установлении взаимозависимости заведомо ложных сообщений об акте терроризма (ст. 207 УК РФ) и терроризма (ст. 205 УК РФ). Сложность решения этой задачи обусловлена тем, что накопленный объем статистического наблюдения недостаточен для получения состоятельных статистических оценок, поскольку не выполняется закон больших чисел. Вместе с тем, задача заключается в аналитическом описании тенденции (тренда) роста заведомо ложных сообщений об акте терроризма в зависимости от террористических актов. Аналитическое решение этой задачи выходит за рамки правового исследования, однако представляет интерес в криминологическом плане. Отметим, что впервые в правовой науке применяемый метод заимствован из теоретической физики и экономики (так называемый «биржевой прогноз»). В этих областях также решаются задачи открытия естественных законов на основе прогнозирования и ретроспекции. Последняя особенно характерна для фондовых бирж, где результаты прогнозов проверяются немедленно и неотвратимо, в силу чего методика работы с ними непрерывно совершенствуется.

Итак, рассмотрена следующая криминологическая задача Статистические данные по ст.ст. 205, 207 УК РФ за период, например (без ограничения общности), 1999–2003 годы имеют вид, показанный в таблице

Год	ст. 205 УК РФ x_i	ст.207 УК РФ y_i
1999	20	3462
2000	135	4035
2001	324	5323
2002	360	6762
2003	561	7811

Необходимо найти количественные ***неслучайные*** характеристики зависимости преступлений, предусмотренных по ст. 207 УК РФ, в связи с преступлениями, предусмотренными по ст.205 УК РФ.

Поскольку малый объём выборки (N=5) ограничивает выбор метода, будем искать зависимость в виде прямой линии $y = b+ax$ по методу наименьших квадратов (уравнение линейной регрессии).

Задача сводится к исследованию следующего функционала:

$$\sum_{i=1}^{i=n}\left[y_i - (ax_i + b)\right]^2 = \min$$, где a и b – искомые величины

Необходимо в общем случае аналитически найти значения характеристик a и b такие, при которых функционал принимает минимальное (экстремальное) значение.

Взяв частные производные по a и b, и приравняв их (частные производные) нулю (необходимое условие экстремума функции) с целью нахождения минимума, получим два уравнения с двумя искомыми неизвестными a и b.

$$\begin{cases} a\sum_{i=1}^{n} x_i^2 + b\sum_{i=1}^{n} x_i - \sum_{i=1}^{n} x_i y_i = 0; \\ a\sum x_i + bn - \sum_{i=1}^{n} y_i = 0; \end{cases}$$

Решение этой системы в общем случае имеет вид:

$$a = \frac{n\sum_{i=1}^{n} x_i y - \sum_{i=1}^{n} x_i \sum_{i=1}^{n} y_i}{n\sum_{i=1}^{n} x_i^2 - (\sum_{i=1}^{n} x_i)^2}$$

$$b = \frac{\sum_{i=1}^{n} x_i^2 \sum_{i=1}^{n} y_i - \sum_{i=1}^{n} x_i \sum_{i=1}^{n} x_i y_i}{n\sum_{i=1}^{n} x_i^2 - (\sum_{i=1}^{n} x_i)^2}$$

Таким образом, неслучайные параметры a и b прямой (тренда преступности) вычисляются исключительно через статистические данные.

В нашем случае получим параметры a и b по числовым данным таблицы :

$$\sum_{i=1}^{5} x_i = 1.4 \times 10^3 \ ; \qquad (\sum_{i=1}^{5} x_i)^2 = 1.96 \times 10^6 \ ;$$

$$\sum_{i=1}^{5} x_i^2 = 5.679 \times 10^5 \ ; \qquad \sum_{i=1}^{5} y_i = 2.739 \times 10^4 \ ;$$

$$\sum_{i=1}^{5} x_i \sum_{i=1}^{5} y_i = 383.5 \times 10^5 \ ; \qquad \sum_{i=1}^{5} x_i \times y_i = 91.533 \times 10^5 \ ;$$

$$a = \frac{5 \times 91.533 \times 10^5 - 383.5 \times 10^5}{5 \times 5.679 \times 10^5 - 19.6 \times 10^5} = \frac{74.165 \times 10^5}{8.795 \times 10^5} = 8.433 \ ;$$

$b = 3117$;

Итак, искомая зависимость (естественный локальный закон) имеет вид:

y = 3117 + 8,433 x

Это уравнение, как аналитическая запись локального естественного закона, позволяет прогнозировать как количество преступлений, предусмотренных ст. 207 УК РФ, в связи с количеством преступлений, предусмотренных ст. 205, так и проводить ретроспективный анализ. Так, согласно статистическим данным (см. таблицу) в 1999г. было зарегистрировано 20 террористических актов (x). Расчет с использованием указанной формулы показал, что количество заведомо ложных сообщений в данный период должно было составлять 3 286 преступлений. Погрешность при этом равна 5,0 %. В 2000г. зарегистрировано 135 актов терроризма, соответственно аналогичный расчет показал, что количество рассматриваемых преступлений должно было составлять 4 255, погрешность равна 5,4% и т.д.

Общая картина расчетов представляется следующим образом:

(x = 20) → y = 3 286 (+176) = 3 462; 5, 0%
(x = 135) → y = 4 255 (- 220) = 4 035; 5, 4%
(x = 324) → y = 5 849 (-526) = 5 323; 9, 8%
(x = 360) → y = 6 152 (+610) = 6 762; 9, 0%
(x = 561) → y = 7 848 (-037) = 7 811; 0, 4%
(x = 700) → y = 9 020; <10%
(x = 800) → y = 9 863; <10%
(x = 0) → y = 3 117 (фоновый уровень заведомо ложных сообщений);
(x =-317) → y ≈ 0 (уровень антитеррористических операций).

Учитывая рост террористических актов, можно определить, какое количество заведомо ложных сообщений об акте терроризма можно ожидать. Так, например, если количество террористических актов достигнет 700, то следует ожидать более 9 020 заведомо ложных сообщений об акте терроризма. При дальнейшем росте – при 800 актах терроризма количество рассматриваемых преступлений может достигнуть 9 863. Описываемый естественный локальный закон позволяет решать задачи интерполяции и экстраполяции и сравнивать теоретически полученные результаты со статистическими данными о заведомо ложных сообщениях об акте терроризма. Особый интерес представляет исследование области определения и области допустимых значений естественного локального закона. Под областью определения понимается временной период, в пределах которого этот закон с приемлемой для практики точностью позволяет установить зависимость заведомо ложных сообщений об акте терроризма от количества террористических актов. Применительно к периоду 1999–2003гг. этот закон является линейным и определяет линейную тенденцию (тренд) роста числа заведомо ложных сообщений об акте терроризма. Однако неясно, будет ли сохраняться линейность, например, до 2010г. или 2020г. или статистические данные следует описывать с помощью нелинейных законов. Кроме того, дополнительного исследования требует определение области допустимых значений прогнозных и ретроспективных оценок, Заслуживает внимания оценка ожидаемого количества заведомо ложных сообщений об акте терроризма при отсутствии террористических актов (фоновый уровень заведомо ложных сообщений об акте терроризма). Практика показывает, что такие явления имеют место. В нашем случае этот фоновый уровень следует из естественного локального закона взаимосвязи терроризма и заведомо ложных сообщений об акте терроризма. При x=0, где x – количество террористических актов, он равен 3 117 преступлений, предусмотренных ст. 207 УК РФ.

В ***заключении*** отмечается, что цель исследования достигнута. В процессе достижения цели поставленные в работе задачи решены и успешно проверены на практике. Получены новые решения актуальных научно-практических правовых задач с положительным эффектом, которые используются в учебном процессе юридических вузов (факультетов) и производственной деятельности кредитных организаций ФК «УРАЛСИБ» и ОАО «РОСБАНК». Положительный эффект обеспечения информационной безопасности достигается в основном за счет применения соответствующих международных стандартов(лучших практик), которые являются механизмами реализации нормативных правовых актов.

По теме диссертации автором опубликованы следующие работы[20]

1. Системный анализ проблем защиты информации в специальных АСУ. / Тезисы докладов на Межведомственном семинаре Минрадиопрома и Минобороны (г. Баку, 23.01.85г.), М.: НИИ АА, 1985 – 0.3 п.л.
2. Системный анализ проблемы защиты информации. М.: Вопросы специальной радиоэлектроники №20, 1985 - 0.4 п.л.
3. Положение о Межведомственном координационном совете по проблемам защиты информации. М.: Комиссия Президиума СМ СССР по военно-промышленным вопросам ,1985 – 0.6/0,3 (в соавторстве с В.С.Семенихиным)
4. Системная защита информации при проведении НИОКР и на объектах заказчика. Курс лекций для руководящего состава Минрадиопрома. М.: Минрадиопром, 1986 – 2.5 п.л.
5. Теоретические основы системной защиты информации. Отчет по НИР «Защита», Книга 1, М.: НИИ АА, 1987 – 4.0 п.л.
6. Системный анализ материалов по защите информации. Отчет по НИР «Защита». Книга II. М.: НИИ АА, 1987–4.0/1.0 (в соавторстве с В.Д. Булановым и др.)
7. Классификация возможных каналов утечки информации. Отчет по НИР «Защита». Книга IV. М.: НИИ АА, 1987 - 5.0/1.0 (в соавторстве с В.Д. Булановым и др.)
8. Классификация средств защиты информации. Отчет по НИР «Защита». Книга V. М.: НИИ АА, 1987 - 6.0/1.0 (в соавторстве с В.Д. Булановым и др.)
9. Специальное обеспечение защиты информации. Отчет по НИР «Защита». Книга VI. М.: НИИ АА, 1987 - 3.0/1.0 (в соавторстве с В.Д. Булановым и др.)
10. Руководство по системной защите информации. Отчет по НИР «Защита». Книга VII. М.: НИИ АА, 1987- 2.0/1.0 (в соавторстве с В.Д. Булановым и др.)
11. Особенности построения информационных систем с учетом конфликтного взаимодействия.// Тезисы докладов Всесоюзной научно-технической конференции «Интегральные информационные системы». М.: ГК ВТИ, 1989 – 0,2 п.л.

[20] Подчеркнуты публикации в рецензируемых научных журналах, депонированные работы и работы, опубликованные в материалах всесоюзных, всероссийских и международных конференциях и симпозиумах в соответствии с п.11 « Положение о порядке присуждения ученых степеней».

12. К правовому государству через правовую информатику. М.: Вузовские вести №9 , 1996 – 0,5 п.л.
13. Адаптация программного администрирования при модернизации корпоративных информационных сетей.// Учебное пособие под редакцией Г.О.Крылова// М.: Академия оборонных отраслей промышленности ,1998–4.0/1,0 (в соавторстве с Ю.И.Чересовым)
14. Интегральная оценка методом главных компонент качества подготовки специалистов юридического профиля // Труды профессорско-преподавательского состава Военного Университета. ВУМО, М.: ВУМО, 2000 – 0,6/0,3 п.л. (в соавторстве с В.М.Селезневым)
15. Сравнение профилей учебных подразделений Военного Университета на основании интегральных оценок // Тезисы доклада на конференции 23 мая 2000г. М.: М.: ВУМО, 2000 – 0,6/0,3 п.л. (в соавторстве с В.М.Селезневым)
16. Сравнение учебных подразделений Военного Университета на основании интегральных оценок, полученных методом главных компонент//Тезисы доклада на конференции «Роль фундаментальных и прикладных технологий в образовании», –М.: ВУМО, 2000 – 0,6/0,3 п.л. (в соавторстве с В.М.Селезневым)
17. Основы информационной безопасности государства на современном этапе М.: ВАГШ, 2000 – 0,3/0.2 п.л. (в соавторстве с Н.И. Турко);
18. Использование хеширования по сигнатуре для поиска по сходству // Бойцов Л.М., Крылов Г.О.// ВМК, МГУ, М.; Прикладная математика и информатика №8 2001 – 0.6/0,3 п.л.
19. Экспериментальное сравнение современных словарных методов поиска по сходству с хешированием по сигнатуре // Бойцов Л.М., Крылов Г.О.;//Тезисы международной конференции «Системный анализ и информационные технологии», Киев, 2001 – 0.4/0,2 п.л.
20. Интернет-технологии и вопросы правового регулирования их использования. М.: Сборник НТИ, серия 1, №9,10.2001 0.3/0,1п.л. (в соавторстве с В.А. Ниесовым и др.);
    http://ilaw.nm.ru/krstol/june/intro.htm
21. Информационно-технологическая политика АБ «ИБГ НИКойл» на 2001-2005 годы.- М.: АБ ИБГ НИКойл, 2001 - 0.6/0,3 п.л. (в соавторстве с В.Н.Ануфриевым);
22. Отчет по НИР «Исследование возможных каналов утечки информации в беспроводных широкополосных сетях передачи данных» (шифр «Лента СП»). г. Санкт-Петербург, Войсковая часть 99727, 2002-6.0/1.0 п.л. (в соавторстве с С.Н.Гаевцом и др.)
23. Отчет по НИР «Рекомендации по защите от утечки информации цифровых АТС» (шифр «Линь КС»).// Секция инженерных

проблем Российской инженерной академии. //г. Санкт-Петербург, 2003 - 6.0/1.0 п.л. (в соавторстве с С.Н.Гаевцом и др.)

24. Проблемы информационной безопасности и их актуальность для военно-медицинской службы //М.: Военно-медицинский журнал, 2003 , №5,- 0,9/0,3 п.л. (в соавторстве с С.Н.Гаевцом и др.)
25. О системе лицензирования и сертификации в области защиты информации // М.:Военно-медицинский журнал, 2003, №6 ,- 0,9/0,3 п.л. (в соавторстве с С.Н.Гаевцом и др.)
26. Обеспечение информационной безопасности на современном этапе развития социально-гигиенического мониторинга // Труды научно-практической конференции «Проблемы профилактики актуальных для войск инфекций и пути их решения», - М., 2003 -,- 0,6/0,2 п.л. (в соавторстве с С.Н.Гаевцом и др.)
27. Международно-правовые проблемы информационной безопасности.- М.: ВАГШ, 2003 – 2.0/1,0 п.л. (в соавторстве с А.Н.Кубанковым)
28. Словарь терминов и определений в области информационной безопасности. - М.: ВАГШ, 2003- 4.0/1,0 п.л. (в соавторстве с С.В. Коротковым и др.)
29. Реализация блочных индексных файлов с применением реляционных СУБД в задачах поиска информации // Бойцов Л.М., Крылов Г.О.; Московская академия рынка труда и информационных технологий- М. 2003,- Деп. в ВИНИТИ 18.04.03, №748-В2003 – 0,3/0,1 п.л.
30. Судебная защита граждан и юридических лиц от воздействия информации, посягающей на честь, достоинство и деловую репутацию, распространенной СМИ // Материалы Всероссийской научно-практической конференции. – М.: Российская академия правосудия, 2003. - 0,4/0,2 п.л. (в соавторстве с Мауриным В.С.)
31. Информационно-правовые отношения оператора Интернет и пользователя Интернет // Право и суд в современном мире: Материалы II ежегодной научной конференции. М.: РАП, 2003. – 0,4/0,2 п.л. (в соавторстве с М.Б.Маношкиным)
32. Особенности дидактического проектирования процедур решения аналитических задач в финансово–экономических вузах //Сб. материалов VII Всероссийской научно- практической конференции «Экономическое обеспечение обороноспособности государства и реформирования ВС». – Ярославль: ЯВФЭИ, 2004 (0,4 п.л./ 0,2 п.л.; соавтор Трофимец В.Я.)
33. Оценка объектов военно-экономического анализа по многоуровенной системе критериев: проблемы, методы, программная реализация// Сб. материалов VII Всероссийской научно- практической конференции «Экономическое обеспечение

обороноспособности государства и реформирования ВС»– Ярославль: ЯВФЭИ, 2004(0,4/0,2 п.л.; соавтор Трофимец В.Я.)

34. Имитационное моделирование автоматизированных процедур поддержки принятия экономических решений // Межвузовский сборник научных трудов « Математика и математическое образование. Выпуск 5». – Ярославль: ЯГТУ, 2004 (0,4 / 0,2 п.л.; соавтор Трофимец В.Я.)
35. Методы и критерии решения задач военно- экономического анализа при производстве продукции по государственному оборонному заказу // Вестник Московской академии рынка труда и информационных технологий,- 2004. – №12 (0,6 / 0,2 п.л.; соавтор Трофимец В.Я. и Чересов Ю.И.)
36. Информационная безопасность государства в информационном обществе. //Учебное пособие для ВВУЗ.// – М.: ВАГШ, 2004 -3,0/ 1,0 п.л. (в соавторстве с Е.А.Дербиным и др.)
37. Латентная преступность в Российской Федерации за 2001-2002гг // Статистический сборник. Министерство юстиции РФ, - М.: РПА МЮ РФ, 2004 – 2,5/0,5 п.л. (в соавторстве с П.Э.Жигоцким и др.)
38. Информационные операции современности. //Учебное пособие для ВВУЗ//- М.:ВАГШ, 2004 - 16,0/4,0 (в соавторстве с Е.А.Дербиным и др.)
39. Организация взаимоотношений субъектов информационной деятельности в процессе предоставления информации о судопроизводстве // Судебная реформа в современной России: Материалы Всероссийской научной конференции. М.: МГЮА: РАП, 2004. – 0,4/0,2 п.л. (в соавторстве с М.Б.Маношкиным)
40. Концепция информационной безопасности Финансовой корпорации «УРАЛСИБ». М.:УРАЛСИБ, 2004 – 1,0 п.л.
41. Положение о Дирекции аудита и методологии информационной безопасности Финансовой корпорации «УРАЛСИБ». М.:УРАЛСИБ, 2004 – 0.8 п.л.
42. Должностные инструкции сотрудников Дирекции аудита и методологии информационной безопасности Финансовой корпорации «УРАЛСИБ». М.:УРАЛСИБ, 2004 – 3.2 п.л.
43. Информационно-правовой статус оператора Интернет // Право и суд в современном мире: Материалы III ежегодной научной конференции. М.: РАП, 2004. – 0,4/0,2 п.л. (в соавторстве с М.Б.Маношкиным)
44. Криминологический анализ взаимосвязи актов терроризма и заведомо ложных сообщений о них, М.: РПА МЮ РФ ,2005 – 0,8/0,4 п.л. (в соавторстве с Г.Л.Куликовой)
45. Сравнительно-правовой анализ регулирования деятельности оператора Интернет // Сравнительно-правовые проблемы:

Сборник научных трудов. М.: РАП, 2005. – 0,4/0,2 п.л. (в соавторстве с М.Б.Маношкиным)

46. Политика информационной безопасности Финансовой корпорации «УРАЛСИБ». М.:УРАЛСИБ, 2005 – 1.0 п.л.
47. Аудит информационной безопасности на основе ключевых областей Концепции безопасности Финансовой корпорации «УРАЛСИБ». М.:УРАЛСИБ, 2005 – 1.0/0,5п.л.(в соавторстве с С.М.Романовским)
48. Создание и регистрация сайта академического правового колледжа РПА МЮ РФ.//Материалы Международных Державинских чтений. М.: РПА МЮ РФ, 2006 – 0,2 /0.1 п.л. (в соавторстве с И.В.Рыбкиным и др.)
49. Правовое обеспечение информационной безопасности потребителей Интернет-услуг//Материалы международных Екатеринских чтений 2006года, М.: НИЕВ, 2006 - 0,2/0,1п.л. (в соавторстве с В.Л.Никитиной)
50. Аксиоматические особенности системы права.// Материалы международных Державинских чтений. М.: РПА МЮ РФ, 2006 – 0.2/0,1 п.л. (в соавторстве с В.Л.Никитиной)
51. Теоретико-правовые аспекты информационной безопасности. Монография. М.: НИЕВ, 2007- 4,0 п.л.
52. Доктринально-нормативное обеспечение информационного превосходства в геополитических информационных операциях, М.: Безопасность информационных технологий №2, 2007- 0,2 п.л.
53. .Международно-правовое регулирование информационной безопасности и его реализация в России. М.: Безопасность информационных технологий №2, 2007- 0,2 п.л.
54. Международно-правовое регулирование информационной безопасности и его реализация в Российской Федерации. М.: Вестник Российской правовой академии №4, 2007- 0,2 п.л. (в печати)

Подписано в печать 04.04.2007 г.
Формат 60х90 $^{1}/_{16}$. Объем 1.5 печ.л. Тираж 100 экз.

Государственное образовательное учреждение
высшего профессионального образования
Московский инженерно-физический институт
(государственный университет)
115409, г. Москва, Каширское шоссе, д.31