МИНИСТЕРСТВО ОБРАЗОВАНИЯ АЗЕРБАЙДЖАНСКОЙ РЕСПУБЛИКИ
БАКИНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

На правах рукописи

РАМИЛЬ МАХИР оглы АСЛАНОВ

ТЕОРЕТИЧЕСКИЕ И КОНСТИТУЦИОННЫЕ ОСНОВЫ ПРАВОВОГО ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ ПОСТРОЕНИИ ИНФОРМАЦИОННОГО ОБЩЕСТВА В АЗЕРБАЙДЖАНСКОЙ РЕСПУБЛИКЕ И РОССИЙСКОЙ ФЕДЕРАЦИИ

Специальность: 5614.01 – «Административное право, финансовое право, информационное право»

А В Т О Р Е Ф Е Р А Т

диссертации на соискание ученой степени доктора юридических наук

БАКУ – 2016

Диссертация выполнена в Российской Правовой Академии Министерства Юстиции Российской Федерации, прошла всестороннее обсуждение и рекомендована к публичной защите.

Научный консультант: **А.В.МОРОЗОВ**
Доктор юридических наук, профессор

Официальные оппоненты: **И.О.КУЛИЕВ**
Доктор юридических наук, профессор

МИНБАЛЕЕВ А.В.
Доктор юридических наук, профессор

Р.В.ИГОНИН
Доктор юридических наук, профессор

Ведущая организация: **Академия Государственного Управления при Президенте Азербайджанской Республики**

Защита диссертации состоится «_01_» « 06_» 2016 года в «_____» часов на заседании Диссертационного совета FD.02.013 при Бакинском Государственном Университете.

Адрес: AZ 1143, г. Баку, улица З. Халилова 23, Бакинский Государственный Университет, первый корпус, аудитория № 901.

С диссертацией можно ознакомиться в библиотеке Бакинского Государственного Университета.

Автореферат разослан «____» «_____» 2016 г.

Ученый секретарь Диссертационного совета FD.02.013, доктор философии по праву: **А.Г. МАМЕДОВ**

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы диссертационного исследования. Мир XXI века уверенно можно назвать эрой информационного общества. Информационные технологии (ИТ) глубоко проникли практически во все сферы жизнедеятельности человека. Быстрое развитие сектора ИТ является одним из актуальных процессов современности, характеризующим новый тип нынешнего общества. Информация сегодня превратилась в стратегический ресурс государства. По степени доступа общества к информационным технологиям судят об уровне общего развития государства.

Азербайджанская Республика и Российская Федерация, традиционно имеющие тесные научные взаимосвязи в различных областях, включая и правовую науку, в эпоху построения информационного общества получили новый импульс для дальнейшего сотрудничества. В рамках Межгосударственного Соглашения между Азербайджанской Республикой и Российской Федерацией предусмотрена подготовка специалистов высшей квалификации, изучающих опыт становления государственных институтов наших стран для укрепления добрососедских отношений, имплементации законодательства, использования положительных примеров правового регулирования важнейших направлений развития государства и общества.

В последние годы вопросам правового обеспечения развития информационного общества в Азербайджанской Республике и Российской Федерации уделяется повышенное внимание, что обусловлено принятием целого ряда международно-правовых документов, таких как Декларация принципов информационного общества, итоговых документов Всемирной встречи на высшем уровне по вопросам информационного общества в Женеве и в Тунисе, а также документов, принятых в их развитие в Азербайджанской Республике и Российской Федерации.

В связи с этим весьма актуальным является изучение и сравнительный анализ правового обеспечения построения информационного общества и важнейшей его составляющей - информационной безопасности. В контексте демократического общества следует отметить и то, что информационная безопасность должна обеспечиваться как обеспечение права свободы. Быстрое развитие компьютерных и интернет технологий делает эту проблему более актуальной. При этом создаются серьезные проблемы в применении закона в отношении гарантии защиты секретности транзакций, т.к. неограниченность государственными границами компьютерных сетей, подключённых к интернету, имеет глобальный характер.

Если национальные правовые системы находятся только в рамках границ, то сведения посредством компьютеров проходят границы бесчисленного количества государств и правовых систем. Неограниченность задачи компьютерной безопасности государственными границами обуславливает международное сотрудничество в этой сфере и развитие в глобальных масштабах закона и применимости закона. Представляется, что правовой анализ указанной проблемы в современной юридической литературе пока еще недостаточно разработан. Однако значительная правотворческая активность последних лет в сфере построения информационного общества дала существенные результаты. В России был принят целый ряд законодательных актов, регулирующих вопросы обработки и использования информации в различных направлениях деятельности: Гражданский кодекс Российской Федерации (часть четвертая) от 18.12.2006 № 231-ФЗ, федеральные законы от 07.07.2003 № 26-ФЗ «О связи», от 29.07.2004 № 98-ФЗ «О коммерческой тайне», от 03.02.2006 № 38-ФЗ «О рекламе», от 26.07.2006 № 135-ФЗ «О защите конкуренции», от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», от 27.07.2006 № 152-ФЗ «О персональных данных», от 22.12.2008 № 262-ФЗ «Об обеспечении доступа к информации о деятельности судов в Российской Федерации», от 09.02.2009 № 8-ФЗ «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления», от 27.07.2010 № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг», от 27.07.2010 № 224-ФЗ «О противодействии неправомерному использованию инсайдерской информации и манипулированию рынком и о внесении изменений в отдельные законодательные акты Российской Федерации», от 28.12.2010 № 390-ФЗ «О безопасности», от 29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию», Федеральный конституционный закон от 07.02.2011 «О судах общей юрисдикции в Российской Федерации», от 06.04.2011 № 63-ФЗ «Об электронной подписи», от 25.07.2011 № 261-ФЗ «О внесении изменений в Федеральный закон «О персональных данных».

В последние годы также утверждены несколько основополагающих документов в сфере развития информационного общества в России, затрагивающие вопросы развития сферы информационной безопасности. Это, прежде всего, «Стратегия развития информацион-

ного общества в Российской Федерации» (Пр-212 от 07.02.2008) и «Стратегия национальной безопасности Российской Федерации до 2020 года» (Указ № 537 от 12.05.2009).

В Азербайджане так же разрабатываются и принимаются законодательные акты, подписываются указы и распоряжения в сфере информационного права: Распоряжение Президента Азербайджанской Республики «Об утверждении Государственной программы по созданию системы биометрической идентификации в Азербайджанской Республике на 2007-2012 годы», Закон Азербайджанской Республики «Об информации, информатизации и защиты информации» от 03.04.1998 года, «Приказ о тарифах за услуги связи» № 249 от 06.09.2001 года с целью развития Интернета, Приказ № 91 от 13.03.2001 года о создании «Bakinternet», Распоряжение Президента Азербайджанской Республики об утверждении «Национальной стратегии по информационным и коммуникационным технологиям во имя развития Азербайджанской Республики (2003-2012 годы)», Распоряжение Кабинета Министров Азербайджанской Республики от 14 мая 2010 года о формировании «Электронного правительства». 20 февраля 2004 года было упразднено министерство связи и Указом Президента от 10 августа 2004 года было сформировано Министерство связи и информационных технологий Азербайджанской Республики. 2013 год был объявлен в Азербайджане «годом информационно-коммуникационных технологий». Распоряжением Президента Азербайджанской Республики от 16 апреля 2007 года №2090 подготовка высококвалифицированных кадров в области ИКТ была признана приоритетным направлением. 2 апреля 2014 года Президентом Азербайджанской Республики была утверждена «Национальная стратегия по развитию информационного общества в Азербайджанской Республике на 2014-2020 годы».

Как следует из Стратегии развития информационного общества в Российской Федерации, совершенствование системы государственных гарантий конституционных прав человека и гражданина при построении глобального информационного общества является одной из задач достижения такой цели, определенной Стратегией, как повышение качества жизни граждан.

В силу указанной специфики общие принципы исследования правового обеспечения информационной безопасности должны быть существенно дополнены развернутым анализом системы знаний конкретных профессиональных информационных ресурсов, отражающих весь комплекс специфических задач, определяющих ее содержание.

Необходимо отметить, что многие аспекты правового обеспечения информационной безопасности также получили более или менее глубокую разработку в целом ряде работ современных авторов. Это не только научные труды, но и учебники, учебные пособия, написанные и изданные в современный период в Российской Федерации и Азербайджанской Республике. Однако фундаментального научного исследования, посвященного разработке теоретико-методологических и правовых основ правового обеспечения информационной безопасности при построении информационного общества в Российской Федерации и Азербайджанской Республике, опирающегося на передовые достижения современной науки, пока не создано. Настоящая диссертационная работа призвана восполнить это пробел.

Актуальность исследования также обусловлена следующими факторами:

– повышением роли и значимости правового обеспечения информационной безопасности в жизни современного информационного общества, что обусловлено ее задачами, а также правами граждан обоих государств, сформулированных в Конституциях республик;

– необходимостью совершенствования конституционных основ и законодательства в исследуемой области;

– значимостью и активизацией деятельности в сфере правового обеспечения информационной безопасности;

– необходимостью разработки теоретической и методологической основы для формирования законодательной базы правового обеспечения информационной безопасности;

– характерной для современной эпохи общей тенденцией повышения значимости профессиональной компетентности, затронувшей, в первую очередь, информационно насыщенные профессии;

– появлением новых вызовов и угроз информационной безопасности в условиях глобализации и построения информационного общества в России и Азербайджанской Республике;

– необходимостью совершенствования универсальных международных основ в исследуемой области;

– особой значимостью вопросов формирования и совершенствования правового обеспечения информационной безопасности в целом для безопасности государства;

– необходимостью своевременного развития и конкретизации принципов и методов, выработанных в ходе исследования правового

обеспечения информационной безопасности, путем их применения к данному научному исследованию, структура которого обусловлена содержанием специфических задач;

– недостаточной разработанностью системных аспектов формирования правового обеспечения информационной безопасности в юридической научной литературе;

– отсутствием фундаментальных теоретических трудов, касающихся особенностей информационных правоотношений в области обеспечения информационной безопасности при построении информационного общества.

Цель диссертационной работы состоит из:

– внесения ясности в теоретико-законодательные вопросы об определении понятия информационного общества, информационных правоотношений, правовых гарантий информационной безопасности при построении информационного общества в Азербайджанской Республике и Российской Федерации, всестороннего освещения анализа норм, посвященных регулированию методологических вопросов правового обеспечения информационной безопасности;

– определения основных элементов информационной безопасности в целях развития законодательства в области построения информационного общества, а также проведения сравнительного исследования законодательств Азербайджанской Республики и Российской Федерации в контексте правовых норм зарубежных стран для разработки концептуальных положений правовых и конституционных основ развития информационного общества в обоих государствах.

Для достижения указанной цели в диссертационной работе были поставлены следующие **задачи**:

– проанализировать новые вызовы и угрозы информационной безопасности при построении информационного общества в России и Азербайджанской Республике;

– исследовать научно-теоретические вопросы правового обеспечения информационной безопасности в России и Азербайджанской Республике;

– определить понятие «информационное общество», исследовать социально-правовую значимость информационного общества в развитых государствах;

– определить функции правового обеспечения информационной безопасности при построении информационного общества, как в России, так и в Азербайджанской Республике;

– провести сравнительно-правовой анализ законодательства Российской Федерации и Азербайджанской Республики в контексте имплементации международно-правовых актов в сфере правового обеспечения информационной безопасности при построении информационного общества;

– определить системы государственных гарантий конституционных прав человека и гражданина при построении глобального информационного общества;

– рассмотреть законодательную политику стран в сфере электронных общений;

– исследовать правовую базу, определяющую ответственность за правонарушения в информационном пространстве;

– рассмотреть нормативно-методическую базу для проведения административной реформы, принятие и применение процедур управления, создание организационных стандартов государственных услуг и административных регламентов;

– исследовать юридические основы информационного общества, прав граждан на получение информации, ее распространение и использование, формирование прозрачного государственного аппарата и аппарата местного самоуправления, электронного государства;

– рассмотреть реализацию проектов по созданию и внедрению процедур управления по результатам деятельности в органах исполнительной власти;

– провести анализ международно-правового регулирования в сфере обеспечения информационной безопасности;

– провести сравнительный анализ правового регулирования обеспечения информационной безопасности различных государств;

– определить направления развития правового регулирования безопасности современных информационных систем;

– исследовать уровень обеспечения информационной безопасности и правового регулирования доступа к информации;

– исследовать проблемы систематизации законодательства в данной области, юридической техники, унификации терминологии и выработать предложения по дальнейшему совершенствованию законодательства в этой сфере деятельности.

Объектом исследования являются общественные отношения, возникающие при построении информационного общества в России и Азербайджанской Республике в части системного анализа правового обеспечения информационной безопасности.

Предметом исследования выступают теоретические вопросы, правовые нормы, практика формирования и развития единого информационного пространства, место, роль, а также состояние правового обеспечения информационной безопасности при построении информационного общества в России и Азербайджанской Республике.

Теоретические основы исследования. При подготовке диссертационной работы были рассмотрены научные труды А. Алдеско, С.С. Алексеева, И.Л. Бачило, Х. Бидголи, И.Ю. Богдановской, А.Б. Венгерова, О.А. Гаврилова, П. Дракера, И.Б. Кардашовой, М. Кастельса, Д.А. Керимова, В.А. Копылова, В.Н. Кудрявцева, П.У. Кузнецова, Г.В. Мальцева, А.В. Морозова, В.Б. Наумова, Ю.А. Нисневича, А.С. Пиголкина, С.В. Полениной, Т.А. Поляковой, Ю.Г. Просвирнина, И.М. Рассолова, Д. Сайчела, А.А. Стрельцова, Н.И. Соловяненко, В.М. Сырых, Л.К. Терещенко, Ю.А. Тихомирова, Э. Тоффлера, А.А. Фатьянова, Т. Форестера, Р.О. Халфиной, К. Шеннона и других.

Такие азербайджанские учёные как Рамиз Мехтиев, Ильгам Рагимов, Расим Алигулиев, Амир Алиев, Фархад Абдуллаев, Зияфет Аскеров, Ханлар Гаджиев, Ровшан Исмаилов и другие своими научными работами внесли значительный вклад в информационное законодательство Азербайджанской Республики.

Первые научные исследования, затрагивающие вопросы совершенствования правового регулирования в области обеспечения информационной безопасности, можно отнести к концу XX века. В них заложены основы методологии изучения проблем формирования правового обеспечения информационной безопасности. Однако всесторонне исследовать проблемы правового обеспечения информационной безопасности при построении информационного общества в России и Азербайджанской Республике в рамках указанных трудов невозможно.

Нормативная база исследования основывается на принципах и теоретических положениях конституционного права, административного права, теории права и государства, информационного права, гражданского права, уголовного права, арбитражного права и т.д. В частности, при подготовке диссертации использовались положения Конституций Российской Федерации и Азербайджанской Республики,

различные конституционные законы, подзаконные акты, а также различные международные акты в исследуемой области.

Методологическая основа и методика исследования. Обобщение нормативных, эмпирических и теоретических источников потребовало применения многоуровневого комплекса методов и принципов познания, присущих современной науке. Так, методологическую основу исследования составили основополагающие положения общей теории, философии и социологии права. При этом фундаментальные положения взяты в единстве с такими общенаучными, специальными и частными методами как диалектический, историко-правовой, сравнительно-правовой, формально-логический, системный анализ, анализ документов, и другими.

Эмпирическую базу исследования составили материалы Советов Безопасности Российской Федерации и Азербайджанской Республики, парламентских слушаний в Российской Федерации и Азербайджанской Республике, заключения группы международных экспертов по международной информационной безопасности и международных организаций.

Научная новизна диссертационной работы состоит в том, что это первая исследовательская работа в Азербайджанской Республике, посвященная комплексному исследованию правового обеспечения информационной безопасности при построении информационного общества в Российской Федерации и Азербайджанской Республике. После принятия законодательных актов в указанной сфере, тема информационной безопасности и защиты прав человека приобретает более актуальный характер, возникает необходимость в разработке концепции правовых основ построения информационного общества.

На защиту выносятся следующие основные **положения, являющиеся новыми или содержащие элементы новизны:**

1. Среди наиболее актуальных угроз информационной безопасности на современном этапе развития общества, которые необходимо регулировать организационно-правовыми решениями, можно выделить следующие:

а) разработка, создание и использование средств воздействия и нанесения ущерба информационным ресурсам и телекоммуникационным системам государства;

б) целенаправленное информационное воздействие на критически важные структуры с применением информационного оружия в отношении военных и гражданских объектов, систем и институтов

государств, нарушение нормального функционирования которых создает прямые угрозы национальной безопасности;

в) информационное воздействие, осуществляемое для подрыва политической, экономической и социальной системы государств, психологической обработки населения с целью дестабилизации общества;

г) несанкционированное вмешательство в информационно-телекоммуникационные системы и информационные ресурсы, а также их неправомерное использование;

д) деятельность международных террористических, экстремистских и преступных сообществ, организаций, групп и отдельных правонарушителей, представляющая угрозу информационным ресурсам и критически важным структурам государств;

е) использование информационных технологий в ущерб основным правам человека;

ж) трансграничное распространение информации, противоречащей принципам и нормам международного права, а также национальному законодательству государств. Режим международной информационной безопасности должен гарантировать запрет на сбор, хранение, использование, передачу и распространение информации о частной жизни человека без его согласия и на ограничение доступа граждан к информации, за исключением случаев, предусмотренных законом.

Все эти перечисленные информационные угрозы Азербайджанская Республика испытывает непосредственно. Азербайджану, уже более 23 лет страдающему от оккупации части своей территории Арменией, навязана информационная война, в рамках которой взломом интернет-ресурсов госструктур, общественных организаций, распространением дезинформации и другими видами киберпреступлений занимаются не только хакеры, но и армянские государственные спецслужбы. Очевидно, что такая ситуация логично приводит к необходимости совершенствования существующих национальных законодательств и созданию универсальной международно-правовой базы, определяющей ответственность за правонарушения в информационном пространстве в отношении не только хакеров, но и государственных спецслужб.

2. Надо отметить, что в работах ученых – юристов двух последних лет приоритетным становится мнение о самостоятельном месте информационного права в качестве комплексной отрасли. В информационном пространстве действуют как национальные, так и иностранные, международные субъекты. Информационное право состоит не

только из норм и институтов ряда основных ветвей внутригосударственного права, но и большого количества международных информационных норм. В период построения информационного общества в правовое поле включаются объекты, которые имеют не только экономическую ценность, но и нематериальные блага, как международное право на информацию, направленные на свободное и полное развитие личности. Международные нормы, регламентирующие международное информационное право, формируют структуру международных договоров, обеспечивая международное сотрудничество и реализацию международного права во внутригосударственном праве.

3. Предмет информационного права составляет информация и связанные с ней информационные отношения, обладающие спецификой при осуществлении прав, обязанностей и определении ответственности в информационной сфере. Специфика информационных отношений определяется юридическими свойствами информационных объектов. К информационным объектам относятся не только информация и информационные объекты, но и информационные ресурсы, элементы информационной безопасности в широком смысле слова.

4. Информационные отношения, как элемент общественных отношений, требуют правовое регулирование в области признания, соблюдения и защиты информационных прав и свобод человека. Информационные отношения являются объективным процессом в информационной сфере, и отражают особенности как публично-правовых, так гражданско-правовых методов регулирования. Информационные отношения, кристаллизируясь в правовых нормах, возникают, развиваются и прекращаются в связи с обеспечением информационных интересов личности, государства в информационной сфере, в связи с защитой информации от несанкционированного доступа, обеспечением состояния защищенности информационных и телекоммуникационных систем, как уже развернутых, так и создаваемых.

5. Состояние информационной безопасности не является в современных условиях статичным, а, наоборот, требует постоянного совершенствования в связи с глобальными вызовами и угрозами, возникающими в наш динамичный «информационный век», их трансграничностью, необычайно быстрым развитием, трансформацией, когда информационные технологии стремительно развиваются и приносят обществу не только благо, но и множество проблем и используются, к сожалению, и в преступных целях. В связи с изложенным, на основе

приведенных различных понятий информационной безопасности автором в данном исследовании предлагается понимать информационную безопасность как состояние защищенности национальных интересов от внутренних и внешних угроз в информационной сфере, состоящих из совокупности сбалансированных интересов личности, общества и государства, соответствующее закрепленным конституционным правам и обязанностям граждан.

6. Правовые нормы, которые регулируют обеспечение информационной безопасности, можно дифференцировать на:

– реализацию конституционных прав и свобод человека и гражданина, а также законных интересов общества и государства в информационной сфере;

– развитие информационно-телекоммуникационной инфраструктуры и обеспечение защиты информации;

– развитие рынка информационных средств, продуктов и услуг;

– обеспечение как национальной, так и международной политики в сфере информационной безопасности.

Специфическими правовыми институтами законодательства в рассматриваемой области являются регулируемые законодательством в области обеспечения информационной безопасности такие наиболее развитые в теоретическом и нормативном отношении виды информации, как «право на информацию», «правовой режим информационных систем», «средства массовой информации», «государственная тайна», «персональные данные», «защита информации» и «информационных систем», «информация ограниченного доступа» и др.

7. В настоящее время система взаимоотношений между участниками в сфере обеспечения информационной безопасности объектов информационной и телекоммуникационной инфраструктуры не имеет должного правового регулирования, складывается порой стихийно на основе рыночных механизмов, что создает условия для неконтролируемого воздействия на них и, в том числе, для злоупотреблений.

На объектах информационной и телекоммуникационной инфраструктуры, в том числе, обеспечивающих деятельность силовых и финансовых структур, широко применяется аппаратное и программное обеспечение иностранного производства, что не всегда соответствует предъявляемым требованиям информационной безопасности.

На основе исследования данной проблемы автор полагает, что в организационно-правовом регулировании нуждаются вопросы:

– определения угроз информационной безопасности критически важных объектов информационно-телекоммуникационной инфраструктуры;

– оценки уязвимости объектов информационно-телекоммуникационной инфраструктуры и объектов информатизации от актов незаконного вмешательства и деструктивных информационных воздействий;

– категорирования критически важных объектов информационно-телекоммуникационной инфраструктуры и объектов информатизации в зависимости от негативных последствий, возникающих вследствие прекращения или нарушения их функционирования;

– разработки требований и реализации мер по обеспечению информационной безопасности критически важных объектов информационной и телекоммуникационной инфраструктуры.

8. Анализ состояния организационно-правового обеспечения в информационной сфере, проведенный в рамках настоящего исследования, позволяет сделать вывод о том, что теоретические и методологические основы государственного регулирования в информационной сфере целесообразно сосредоточить в едином документе концептуального характера, определяющим развитие информационного законодательства и позволяющим максимально учесть его состояние, отразив новеллы, включая новые правоотношения и вопросы, с учетом стратегий развития информационного общества в Российской Федерации и Азербайджанской Республике, разработанных концепций развития законодательства, и ряда других правовых документов, касающихся построения информационного общества и развития информационного законодательства.

В диссертационной работе на основе системного анализа информационного законодательства в целях совершенствования правового обеспечения информационной безопасности доказывается необходимость разработки сводного кодифицированного законодательного акта – «Информационного кодекса», как высшей формы систематизации законодательства. Это особенно важно в период построения информационного общества, характеризующегося возникновением новых общественных отношений.

9. В диссертационном исследовании анализированы развитие правовых основ информационного общества в Российской Федерации и Азербайджанской Республике. Анализ нормативных правовых актов позволил сформулировать основные направления развития информа-

ционного общества и сферу деятельности уполномоченных органов государственной власти по реализации этих направлений:

– улучшение качества жизни граждан и условий развития бизнеса в информационном обществе;

– повышение эффективности государственного управления путем построения электронного государства;

– развитие отечественного рынка информационных и телекоммуникационных технологий;

– формирование инфраструктуры информационного общества;

– обеспечение безопасности в информационном обществе;

– создание цифрового контента культурного наследия и предоставление доступа к нему через интернет.

10. Среди нерешенных проблем в сфере обеспечения права на доступ к информации отмечается отсутствие единого нормативного правового акта, закрепляющего основные права граждан и организаций в области доступа к информации, основные принципы предоставления информации и механизм реализации права на доступ к информации; четкой регламентации задач и функций органов государственной власти при формировании открытых государственных информационных ресурсов и обеспечения доступа к ним граждан и организаций; а также единого порядка информационного обмена органов государственной власти с гражданами и организациями посредством использования информационных систем общего пользования.

11. Сравнительно-правовой анализ основных направлений правового обеспечения построения информационного общества в Азербайджанской Республике и Российской Федерации позволил выявить его приоритетные направления:

а) развитие государственной информационной системы и портала государственных и муниципальных услуг;

б) создание и развитие информационных систем поддержки малого и среднего предпринимательства;

в) обеспечение перехода на предоставление государственных и муниципальных услуг в электронном виде;

г) оптимизация порядка исполнения государственных функций и услуг для целей их перевода в электронный вид;

д) разработка механизмов, позволяющих использовать мобильные устройства для доступа к сервисам электронного правительства и банковской системы;

е) развитие сервисов взаимодействия граждан с органами государственной власти при помощи сети интернет;

ж) обеспечение открытости информации о деятельности органов государственной власти и доступности государственных информационных ресурсов для граждан и организаций;

з) создание универсального конструктора официальных сайтов, обеспечивающего разработку, функционирование, контентную и аппаратно-программную поддержку государственных интернет-проектов, не требующих специализированного образования от администраторов сайтов;

и) создание сервисов для обеспечения общественного обсуждения и контроля за деятельностью органов государственной власти, создание инструментов общественного управления на муниципальном уровне;

к) создание и внедрение комплексных информационных систем в области здравоохранения;

л) развитие электронных сервисов для повышения качества оказания услуг в области образования и науки;

м) социальная адаптация и развитие творческих способностей лиц с ограниченными возможностями здоровья посредством использования современных информационных технологий и дистанционных образовательных технологий;

н) совершенствование контрольно-надзорных и разрешительных функций и оптимизация предоставления государственных услуг в сфере здравоохранения, социального развития, санитарно-эпидемиологического благополучия и потребительского рынка, в области градостроительной деятельности и сельского хозяйства за счет использования информационных технологий.

12. В целях развития информационного общества в Российской Федерации и Азербайджанской Республике с учетом анализа состояния правового регулирования в области обеспечения информационной безопасности обосновывается необходимость разработки концепции правовых основ информационного общества наших стран, включая вопросы партнерства государства, бизнеса и гражданского общества в рассматриваемой сфере. В соответствии с направлениями развития информационного общества разработаны конкретные предложения по реализации первоочередных задач правового обеспечения информационной безопасности в Российской Федерации и Азербайджанской Республике. Сформулированы первоочередные меры по совершенствованию правового обеспечения информационной безопасности.

13. Сравнительно-правовой анализ правового обеспечения информационной безопасности Российской Федерации и Азербайджанской Республики показал сходство правовых норм регулирования данной сферы деятельности. Российская Федерация, по мнению автора, дальше продвинулась в развитии законодательства об электронной подписи и электронном документообороте, Азербайджанская Республика же имеет значительные успехи и более продвинулась в вопросах регулирования электронной торговли.

14. Автор предлагает свою концепцию относительно систематизации законодательства. Обосновывается вывод о необходимости разработки законодательства, где будут учитываться современные тенденции развития правового регулирования в области обеспечения информационной безопасности, гласности, приоритета международно-правовых актов, единства информационного пространства, комплексного характера информационных отношений и т.д.

15. На основе изучения законодательной практики зарубежных стран в информационной сфере, обоснован вывод о необходимости дальнейшей имплементации положений универсальных международных правовых актов. Учитывая тот факт, что информационная безопасность непосредственно связана с национальной безопасностью, государства неохотно идут на имплементацию международных норм в области обеспечения международной информационной безопасности. Такое действие (бездействие) есть нарушение прав и свобод человека.

16. Приоритетная роль международных актов связана и с тем фактором, что сегодня происходит интернационализация информационной сферы. Международную информационную безопасность можно обеспечить только путем унификации национально-правовых норм. Существует необходимость преподавания международного информационного права. Глобальные информационные процессы, развитие электронно-телекоммуникационных систем требуют совершенствование ее научного регулирования. Принципиальное значение в данной сфере имеет международное право и международное информационное право.

17. Проведенный автором анализ правонарушений в сети Интернет позволил выявить наиболее типичные из них и сформулировать предложения по совершенствованию административного и уголовного законодательств для эффективного пресечения таких правонарушений и преступлений в сфере информационной безопасности, как:

– подмена адресов отправителя в электронных письмах;

– использование результатов работы вредоносных программ, которые собирают список электронных адресов пользователей и отсылают эту информацию мошенникам;

– использование способов имитации на подставных сайтах;

– использование символики известных компаний в фишинговых письмах;

– отвлечение внимания пользователя заполнением бессмысленных анкет на подставных сайтах, целью которых является не получение статистики, а приватная информация;

– запугивание пользователя ложными сообщениями о скорой блокировке или закрытии банковского счета.

Теоретическая значимость исследования. Предложения и рекомендации автора могут быть использованы в развитии информационного права, совершенствовании теоретической базы законодательства в области обеспечения информационной безопасности, систематизации научно-исследовательских знаний об информационном обществе.

Практическая значимость исследования заключается в том, что ее результаты могут быть использованы для совершенствования законодательства Азербайджанской Республики в области правового обеспечения информационной безопасности при построении информационного общества. Кроме этого, отдельные положения диссертации могут быть использованы при разработке концепции Единого общеевропейского регистра нормативных актов, концепции Единого реестра правовых документов Содружества Независимых Государств и Положения об указанном реестре. Содержащиеся в диссертации положения могут быть также использованы в учебном процессе Российской Правовой Академии Министерства юстиции Российской Федерации и Бакинского Государственного Университета при обучении по специальности «Правоведение» бакалавров по ряду дисциплин («Информационное право», «Правовая информатика» и др.) и магистров по специализации «Информационное право».

Апробация результатов исследования обеспечивалась в теоретической части работы опорой на апробированные методологические и теоретические положения, анализом научных публикаций по всему исследуемому кругу проблем, прямо или косвенно связанных с темой исследования; в эмпирической части — собственным опытом научно-педагогической деятельности автора.

Настоящая диссертация обсуждалась в Российской Правовой Академии Министерства юстиции Российской Федерации, а также на научном семинаре Диссертационного совета, созданного при Бакинском Государственном Университете. Основные положения докторской работы опубликованы автором в монографиях, учебно-методических пособиях, в более чем сорока научных статьях в изданиях, входящих в перечни ВАК при Президенте Азербайджанской Республики, Российской Федерации, Украины, Молдовы, в том числе, одна статья взята к опубликованию в журнале с импакт-фактором из списка Web of Science («The Computer Law & Security Review»).

Отдельные положения докторской диссертации были изложены также в материалах различных международных конференций («Направления и этапы развития информационного права», Москва, 2009; «История и развитие правовой информатизации», Москва, 2010; «Развитие правового обеспечения информационной безопасности», Баку, 2014; «Роль Гейдара Алиева в развитии юридической науки и образования Азербайджанской Республики», Баку, 2015 и др.).

Структура диссертации. Диссертационная работа состоит из введения, пяти глав, заключения и списка использованной литературы.

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Во Введении диссертационной работы обоснована актуальность темы исследования, определены цели и задачи исследования, его методологические и теоретические основы, обоснована научная новизна исследования, приведены сведения о новых научных положениях, представляемых к защите и их практическом значении, об апробации результатов исследования и структуре диссертации.

Первая глава диссертации **– «Угрозы в информационной сфере и теоретические основы правового обеспечения информационной безопасности»,** состоит из трех параграфов.

В первом параграфе – «**Современные угрозы информационной безопасности и пути их устранения»,** анализируются угрозы информационной безопасности современности. Автором отмечено, что мировая информационно-технологическая революция радикально изменила политику, экономику и социальную жизнь мирового сообщества. Возрастающее значение информации и развитие информационных технологий, их роль в современной жизни общества являются несомненными достижениями в этой области. Проблема противодействия использованию потенциала информационно-телекоммуникационных технологий для нанесения ущерба интересам граждан, общества и государства, подготовки и осуществления террористических актов, распространения пропаганды терроризма и насильственного экстремизма является особенно актуальной в связи с необходимостью обеспечения государственно-правовой защиты конституционных прав и свобод человека и гражданина. Кибермир создал безкоординатную способность применять клеветнические комментарии для очернения чести другого человека и отражения этого во всем мире. Кибермошенничество является одним из самых глобальных проблем в мире интернета. С развитием интернета роль информационных технологий в период военных действий возросла в кратном количестве. Общение с интернетом приносит не только пользу и удовольствие. Даже опытного пользователя подстерегает немало опасностей, способных отнять у него и нервы и время, а часто и деньги. Компьютерные злоумышленники используют интернет для похищения информации, извлечения незаконной прибыли, причинения вреда конкурентам. Огромный вред пользователем приносит мошенничество в сети интернета. Под мошенничеством в сети интернета подразумевается: кража личных конфиденциальных данных, выманивание крупных сумм денег. По крайней мере, различаются 2 вида компьютерных преступлений. В первой категории преступлений объектом посягательства является компьютер, и они осуществляются посредством атак на секретность и полноту интернета. А ко второй категории преступлений относятся осуществляемые посредством компьютера мошенничество, кража, подделка. Мошенники для выполнения своих корыстных целей зачастую используют методы социальной инженерии, фишинг, фарминг, вредоносные программы, рассылку спама и т.д.

Среди наиболее актуальных угроз информационной безопасности на современном этапе развития общества можно выделить следующие: разработка, создание и использование средств воздействия и нанесения ущерба информационным ресурсам и телекоммуникационным системам государства, целенаправленное информационное воздействие на критически важные структуры, информационное воздействие, осуществляемое для подрыва политической, экономической и социальной системы государств, психологической обработки населения с целью дестабилизации общества, несанкционированное вмешательство в информационно-

телекоммуникационные системы и информационные ресурсы, а также их неправомерное использование, использование информационных технологий и средств в ущерб основным правам и свободам человека, реализуемым в информационной сфере, трансграничное распространение информации, противоречащей принципам и нормам международного права, а также национальному законодательству государств.

Все эти перечисленные информационные угрозы Азербайджанская Республика испытывает непосредственно. Особенность подобного рода правонарушений состоит в том, что потерпевший может находиться в одной стране, а совершивший преступление – в другой. Интернет придает такому виду преступности транснациональный характер. Азербайджану, уже более 23 лет страдающему от оккупации части своей территории Арменией, навязана информационная война, в рамках которой взломом интернет-ресурсов госструктур, общественных организаций, распространением дезинформации и другими видами киберпреступлений занимаются не только хакеры, но и армянские государственные спецслужбы. Очевидно, что такая ситуация логично приводит к необходимости совершенствования существующих национальных законодательств и созданию универсальной международно-правовой базы, определяющей ответственность за правонарушения в информационном пространстве в отношении не только хакеров, но и государственных спецслужб.

В первом параграфе автором рассматриваются также правовые средства устранения угрозы информационной безопасности. Изучены нормативно-правовые акты Азербайджанской Республики, посвященные информационной безопасности и его обеспечению. Конституция Азербайджанской Республики 1995 года, Закон Азербайджанской Республики «Об информации, информатизации и защите информации» от 3 апреля 1998 года, Закон «О национальной безопасности» от 3 августа 2004 года, а также Законы «О свободе информации», «О средствах массовой информации», «О государственной тайне», «Об электронном документе и электронной подписи», «Об электронной торговле», «О получение информации», «О телекоммуникациях», «О коммерческой тайне», Концепция «Национальной безопасности Азербайджанской Республики» (2007) и т.д. определяют основные приоритеты в сфере информационной безопасности. В 2005 году были приняты поправки в Кодекс об административных правонарушениях и в Уголовный кодекс Азербайджанской Республики, предусматривающие применение штрафных санкций и уголовного наказания за нарушение защиты базы данных. Учитывая трансграничный характер киберпреступности, Азербайджанская Республика осуществляет эффективное международно-правовое сотрудничество с другими государствами. В 2008 году Азербайджанская Республика подписала Конвенцию «О киберпреступности» Совета Европы, а 1 июля 2010 года ратифицировала данную конвенцию.

Приняты специальные нормативно-правовые акты, посвященные угрозам информационной безопасности и его обеспечению, и в Российской Федерации. Определенным импульсом для дальнейшего развития законодательства Российской Федерации в области обеспечения информационной безопасности является принятие в 2006 году Федерального закона «Об информации, информационных технологиях и о защите информации». Однако проблемы установления ответственности за совершение противоправных деяний в информационной сфере требуют своего решения в различных отраслях законодательства. Правовые нормы, направленные на противодействие распространению экстремистской и террористической информации и устанавливающие ответственность за осуществление такой деятельности, содержатся также в Федеральных законах от 07.07.2003 г. «О связи» (статьи 13, 29-40); Кодексе Российской Федерации об административных правонарушениях (статьи 20.3, часть1 статьи 20.27, статья 20.28); Уголовном кодексе Российской Федерации (статьи 205, 205.1, 205.2, 280, 282, 282.2). Как средство или способ совершения преступления, а также средство связи, глобальные компьютерные сети могут использоваться при подготовке и совершении преступлений, предусмотренных статьями 206, 208, 211, 272-274, 277 Уголовного кодекса Российской Федерации и рядом других. Киберпреступления являются преступлениями международного характера: в отдельности государствам не под силу противодействовать киберпреступности.

Все страны мира активно участвуют в создании новых законодательных актов. В последнее время в целом ряде государств национальное законодательство дополнено нормами, направленными на ограничение распространения незапрашиваемых электронных сообщений или запрет этой деятельности. Среди разновидностей хакерских атак быстро набирают популярность так называемые DDoS-атаки, т.е. множество запросов от огромного числа компьютеров со всего мира, зараженных вирусами. В большинстве европейских стран и США приняты специальные акты, прямо и недвусмысленно определяющие хакерские атаки и ответственность за их реализацию. В российском законодательстве эти вопросы должным образом не урегулированы. Наиболее близкие статьи Уголов-

ного кодекса Российской Федерации: статья 272 «Неправомерный доступ к компьютерной информации» и статья 273 «Создание, использование и распространение вредоносных программ для ЭВМ» с максимальными сроками наказания пять и семь лет соответственно. Указанные статьи Уголовного кодекса в случае с DDoS практически не работают. В ходе атаки неправомерного доступа не совершается, а факт использования вирусов вообще недоказуем. Аналогичная ситуация была характерна и для законодательства Азербайджанской Республики до принятия изменений и дополнений, внесенных Законом от 29 июня 2012 года в главу 30 (Киберпреступления) Уголовного кодекса. Несмотря на некоторые пробелы регламентации, законодатель Азербайджанской Республики максимально трансформировал нормы Будапештской конвенции Совета Европы «О киберпреступности» (от 23 ноября 2001 года) в отличие от России, отказавшейся от подписания указанной конвенции. Как известно, Россия настаивает на разработке и принятии новой универсальной конвенции о киберпреступности под эгидой ООН.

Следует отметить, что в дальнейшем, учитывая трансграничность этих угроз, борьба с DDoS неминуемо выйдет на глобальный уровень. Но до сих пор в международных актах и в национальном законодательстве отсутствуют четко сформулированные понятия киберпреступности, кибербезопасности и кибертерроризма. Представляется, что объединение общих усилий международного информационного сообщества необходимо для выработки единого правового механизма регулирования противодействия использованию информационных технологий в преступных целях. Как показывает системный анализ законодательства в данной области, в настоящее время принят уже большой массив нормативных правовых актов, касающихся обеспечения информационной безопасности. Однако целый ряд важнейших для общества вопросов, относящихся к информационной безопасности, до сих пор не имеет соответствующего законодательного урегулирования.

Во втором параграфе первой главы – «**Понятие информационной безопасности и ее роль в развитии информационного общества»,** рассматриваются проблемы перехода к информационному обществу. Переход к информационному обществу составляет основное содержание национальных интересов, закрепленных в нормативно-правовых актах. Принят ряд концептуальных, доктринальных и программных документов по развитию отдельных составляющих информационной инфраструктуры, совершенствованию системы управления

наукой и системы образования, внедрению информационных технологий в деятельность органов государственной власти, использованию информационных технологий в важных областях деятельности человека, общества и государства.

Информационная безопасность страны традиционно рассматривается с двух взаимосвязанных аспектов: технического и социального. Технический аспект подразумевает обеспечение безопасности национальных информационных ресурсов, информационных систем, соответствующей инфраструктуры от несанкционированного доступа, использованных для обеспечения целостности, конфиденциальности и доступности информации.

Социальный аспект заключается в обеспечении защиты национального информационного пространства и систем распространения массовой информации от целенаправленного негативного информационного и организационного воздействия, способного причинить ущерб национальным интересам государства. Развивается система правового регулирования отношений, связанных с созданием и использованием информационных технологий. Однако сохраняется зависимость российской и азербайджанской информационной инфраструктуры от зарубежных информационных технологий вследствие невысокой конкурентоспособности продукции отечественной микроэлектронной промышленности, телекоммуникационного оборудования, средств вычислительной техники и программных продуктов. Более 95% всех информационных и телекоммуникационных систем, эксплуатируемых в Российской Федерации, создано на базе зарубежных информационных технологий. Как показывает мировой опыт постиндустриального развития, важным фактором интенсификации формирования информационного общества является объединение усилий и ресурсов государства, общества и бизнеса для достижения общепризнанных целей – повышения конкурентоспособности страны, благосостояния и качества жизни ее граждан, укрепления обороноспособности и безопасности.

Целью формирования и развития информационного общества в Российской Федерации является повышение качества жизни граждан, развитие экономической, социально-политической, культурной и духовной сфер жизни общества, совершенствование системы государственного управления на основе использования информационных и телекоммуникационных технологий, а также обеспечение конкурентоспособности России.

Национальные интересы Азербайджана в информационной сфере заключаются в соблюдении конституционных прав и свобод граждан в области получения информации и пользования ею, в развитии современных телекоммуникационных технологий, в защите государственных информационных ресурсов от несанкционированного доступа. Информационная безопасность при построении информационного общества является важной, неотъемлемой составляющей национальной безопасности, пронизывающей все сферы жизнедеятельности человека, общества и государства. В рамках настоящего исследования автор полагает, что обеспечение информационной безопасности, так же как и обеспечение национальной безопасности в целом, следует рассматривать как сложную многоуровневую функциональную составляющую системы национальной безопасности в информационной сфере, включающую совокупность взаимосвязанных развивающихся таких составляющих, как национальные интересы, вызовы и угрозы национальным интересам, система обеспечения информационной безопасности.

Таким образом, для обеспечения информационной безопасности при построении информационного общества важнейшее значение имеет разработка нового стратегического документа о национальной безопасности концептуального характера и разработка на государственном уровне законопроекта о национальной безопасности, поскольку в современной правовой системе нуждаются в законодательном закреплении такие глубоко проработанные, научно обоснованные современные понятия, как «национальная безопасность», «национальные интересы», «угрозы национальной безопасности», «обеспечение национальной безопасности», «система национальной безопасности», а также необходимые правовые механизмы противодействия новым вызовам и угрозам информационной безопасности государства.

В третьем параграфе первой главы – «**Проблемы методологии правового обеспечения информационной безопасности»,** изучается взаимосвязь права и информации. С развитием информационных отношений возникли новые концепции относительно правового регулирования. Основу этих концепций составили различные системообразующие критерии. Наличие государственного или общественного интереса, предмет и метод правового регулирования, правоотношения, принципы и источники правового регулирования, научно-технический прогресс и т.д. выдвинуты в качестве системообразующих элементов информационного права. В качестве системообразующих факторов

при образовании отраслей права, кроме предмета и метода правового регулирования, следует выделить и такие, как принципы и функции отрасли права, юридический режим, а применительно к отрасли законодательства - также функции государства.

Интерес государства в формировании информационного права находит свое яркое отражение в проведении государственной политики в области внедрения информационных технологий и построении информационного общества, основные положения которой изложены в законодательстве. Информационные правоотношения регулируются информационно-правовыми нормами. Информационное правоотношение является средством перевода общих установлений информационных правовых норм в конкретные (субъективные) права и обязанности участников отношений в информационной сфере. Предмет правового регулирования информационно-правовой деятельности носит комплексный характер, так как пронизывает все срезы правовой системы: частное и публичное, материальное и процессуальное, внутригосударственное и международное. Это позволяет сделать вывод, что этим, прежде всего, определяются особенности методов правового регулирования в информационной сфере. Возникают новые отрасли права, которые обособляются пока что больше по своему предмету, а метод регулирования для этих отношений может еще вырабатываться, может быть смешанным или вообще не иметь четкого содержания. Это в полной мере можно отнести и к информационному праву как новой отрасли права.

Становление информационного права является длительным процессом. Научные исследования в области информационного права впервые появились в юридической науке в 60-70 годы XX столетия. При этом были использованы разные названия информационного права: «компьютерное право», «правовая кибернетика», «программное право», «программная информатика», «информационно-компьютерное право», «телекоммуникационное право», «информационное право». Ныне в этот список добавлены термины «международное информационное право», «международное телекоммуникационное право», «международное право интернета», «международное право массовой информации» и т.д.

Учитывая множество объективных факторов, особенно, наличие общего предмета правового регулирования, конституционных положений, базовых законов и большого числа норм, касающихся данной сферы и содержащихся в других нормативных правовых актах в различных отраслях права и законодательства, норм международного

права, актуальность задач экономического, социального и политического развития и других, можно утверждать, что информационное право сформировалось как самостоятельная отрасль права.

Вторая глава диссертации – **«Методы правового регулирования информационной безопасности при построении информационного общества»,** состоит из трех параграфов.

В первом параграфе – **«Международное правовое регулирование в сфере обеспечения информационной безопасности»,** исследуются основные международные договоры и документы в области обеспечения информационной безопасности.

Важную роль в развитии законодательства в информационной сфере и в области обеспечения информационной безопасности сыграло принятие в 1948 году Генеральной Ассамблеей ООН Всеобщей декларации прав человека. Информационные права и свободы были развиты в Конвенции Совета Европы о защите прав человека и основных свобод 1950 года и Международном пакте о гражданских и политических правах 1966 года и в других международных актах. Рассматриваемые международные документы устанавливают способы получения и распространения информации. Отмечается, что получение и распространение информации реализуются без какого-либо вмешательства со стороны государственных органов, независимо от государственных границ и распространяются на всякого рода информацию (статья 10 Конвенции, статья 19 Международного пакта). Информационные права и свободы были провозглашены в развитие фундаментальных прав человека.

Начиная с 2000 года, в информационной сфере принят ряд таких основополагающих международных документов, как Окинавская хартия глобального информационного общества, итоговые документы Всемирной встречи на высшем уровне по вопросам информационного общества (2003 г. в Женеве и 2005 г. в Тунисе), которые являются политико-правовыми документами, направленными на ускорение формирования постиндустриальных тенденций в экономической, социально-политической и духовной сферах жизни общества.

23 ноября 2005 года Генеральной Ассамблеей ООН принята Конвенция об использовании электронных сообщений в международных договорах. С 16 января 2006 года она открыта для подписания государствами и направлена на повышение эффективности коммерческой деятельности, открывает новые возможности во взаимной торговле для ранее удаленных друг от друга сторон и рынков, создает единообразные

правила, направленные на устранение барьеров для использования электронных сообщений в международных договорах. Советом Европы и его Комитетом министров был принят ряд актов по обеспечению прозрачности деятельности публичной администрации, по обеспечению свободы мнений в СМИ. В целях международного обмена законодательством была принята Европейская конвенция об информации относительно иностранного законодательства от 07.06.1968г., которая предусматривает, что стороны обязуются предоставлять друг другу информацию о своем законодательстве и процедурах в гражданской и коммерческой сферах, а также судебной системе.

8 мая 1979 года Европейский Парламент принял Резолюцию «О защите прав личности в связи с прогрессом информатики». Советом Европы принята Рекомендация Комитета Министров Совета Европы R(1994)13 «О мерах по обеспечению транспарентности средств массовой информации». Этот документ определяет, что «общественность должна иметь возможность доступа на справедливой и непредвзятой основе к некоторым основным сведениям о СМИ». Принимая во внимание, что цель транспарентности СМИ заключается в том, чтобы каждый мог знать, кто реально владеет тем или иным СМИ, дабы иметь возможность формировать мнение по отношению к распространяемой этими СМИ информации, в Рекомендации вполне обоснованно прописывается особый правовой режим «прозрачности» именно электронных СМИ.

В международных правовых актах также особое внимание уделяется вопросу борьбы с правонарушениями в информационной сфере. В середине 1980-го года была проектирована рекомендация Комитета Экспертов по компьютерным преступлениям Совета Европы о требовании адекватного и быстрого ответа киберпреступлениям и развития международно-правового сотрудничества посредством гармонизации существующего законодательства стран Европейского Союза. В 1997 году министры Внутренних Дел и Юстиции Большой Восьмёрки (G8) встретились в Вашингтоне и приняли сборник принципов против компьютерных преступлений как План Деятельности в отношении борьбы с компьютерными преступлениями. План Деятельности Большой Восьмёрки оказал достаточно важное влияние, и на основе этого Совет Европы подписал Конвенцию о киберпреступлениях от 23.11.2001 года , вступившую в силу 1 июля 2004 года. В настоящее время Конвенцию подписали около 40 государств и лишь 12 ее ратифицировали. Конвенцией предусмотрено, что стороны на взаимной основе оказывают друг другу по возможности

максимально правовую помощь в целях проведения расследований или судебного разбирательства в связи с уголовными преступлениями, связанными с компьютерными системами и данными, или сбора доказательств по уголовному преступлению в электронной форме.

Основные принципы законодательного регулирования общественных отношений в сфере международной информационной безопасности сформулированы в основополагающих международных документах и, как показывает их анализ, являются общепризнанными и приоритетными в развитии информационного законодательства и для наших стран.

Только принятие скоординированных мер на международном уровне позволит адекватно противостоять современным вызовам и угрозам информационной безопасности. При этом среди возможных направлений сотрудничества предполагается содействие разработке международной правовой базы сотрудничества и выработка единого понятийного аппарата в сфере обеспечения информационной безопасности. Для этого необходимо законодательное признание международных договоров источником правового регулирования.

Во втором параграфе второй главы – «**Опыт правового регулирования обеспечения информационной безопасности государств»,** рассматривается зарубежный опыт правового регулирования в сфере обеспечения информационной безопасности. Как показывает анализ зарубежного опыта правового обеспечения информационной безопасности, более 100 государств приняли законы о праве на информацию. Один из старейших - Закон о свободе печати, принятый в Швеции еще в 1776 году, предусматривает право доступа граждан к информации о деятельности органов государственной власти, и сфера его действия распространяется на все виды документов, включая электронные. В Финляндии такой закон был принят в 1951 году. В последние 20 лет такие законы были приняты во Франции, Греции, Дании, Голландии, Бельгии, Португалии, Испании, Финляндии и Италии. Законы о доступе граждан к правительственной информации приняты в США, Канаде, Австралии и Новой Зеландии. В ряде стран Европы, таких как Нидерланды, Испания, Португалия, Австрия, Венгрия, Эстония, Бельгия и Румыния, право граждан на доступ к официальной информации закреплено конституционно. Во Франции, Греции и Италии – эти права закреплены в законах. Совершенствование законодательства в данной сфере продолжается в Великобритании, Германии, Эстонии, Молдове, Польше и ряде других государств.

Анализ показывает, что нормативные правовые акты, регулирующие защиту информации, информационной техники и технологий, направленные на создание и защиту информационных сетей, устанавливающие единые условия использования линий связи и коммуникационных услуг, действуют уже в целом ряде государств. Что касается коммерческой информации, то такие законодательные акты приняты в Великобритании, Франции, США, Канаде и многих других. В США ключевую роль в области обеспечения информационной безопасности играет Закон об электронном государстве 2002 года, а также Закон об информационной безопасности 1987 года. Согласно этим законам, все операторы информационных систем, содержащие конфиденциальную информацию, должны сформировать планы обеспечения информационной безопасности. В 1998 году в США был принят «Акт о защите авторских прав в цифровом тысячелетии», которым введена ответственность, в том числе и уголовная; в то же время в нем предусмотрено ограничение ответственности хост-провайдеров за размещение на их серверах информации, нарушающей чьи-либо авторские права, а также за постановку ссылок на такие ресурсы.

В «Законе о свободе информации» США, в частности, содержится восемь оговорок, согласно которым разглашению не подлежат следующие виды информации: информация о национальной безопасности (ст. 143); информация, представляющая собой коммерческую тайну (ст. 145); информация, разглашение которой запрещено согласно другим законам (ст. 147); информация, разглашение которой нарушило бы ход уголовного расследования или обвинения (ст. 148); информация о состоянии финансовых учреждений (ст. 149); информация геологического и геофизического характера (ст. 150). Причем толкование этих оговорок по американскому праву весьма строгое, с презумпцией в пользу разглашения информации.

Проведенный анализ международных и зарубежных правовых актов в информационной сфере свидетельствует о том, что имеется значительный и разнообразный опыт правового регулирования вопросов доступа к информации как на международном, так и на национальном уровнях. Следует отметить, прежде всего, практику зарубежных государств, где регулируются вопросы доступа к публичной (правительственной информации), которая, однако, в большинстве случаев понимается широко, как всякая информация, находящаяся в распоряжении государственного сектора. Информационная безопасность в

силу глобального характера сетей связи может быть обеспечена лишь при международном взаимодействии. Сравнительный анализ законодательства показывает, что правовое регулирование информационной безопасности наиболее эффективно, когда сформированы правовые основы информационного общества.

В третьем параграфе второй главы – «**Развитие направлений правового регулирования безопасности современных информационных систем»,** раскрывается развитие направлений правового регулирования безопасности современных информационных систем. Отмечается, что концептуальное решение проблемы обеспечения информационной безопасности критически важных объектов в условиях демократического общества, множественности хозяйствующих субъектов с различными организационно-правовыми формами, отношением к собственности и высокой степенью самостоятельности в принятии управленческих решений, требует сбалансированного системного подхода к правовому регулированию этой сферы деятельности. Вышеизложенное, по мнению автора, обосновывает необходимость принятия закона «Об особенностях обеспечения информационной безопасности критически важных объектов информационной и телекоммуникационной инфраструктуры» для установления организационно-правовых особенностей обеспечения информационной безопасности критически важных объектов информационной и телекоммуникационной инфраструктуры различных видов собственности и установления форм и методов государственного регулирования ее обеспечения.

На основе исследования данной проблемы автор полагает, что нуждаются в правовом регулировании следующие вопросы:

– определение угроз информационной безопасности критически важных объектов информационно-телекоммуникационной инфраструктуры;

– оценка уязвимости объектов информационно-телекоммуникационной инфраструктуры и объектов информатизации от актов незаконного вмешательства и деструктивных информационных воздействий;

– категорирование критически важных объектов информационно-телекоммуникационной инфраструктуры и объектов информатизации в зависимости от негативных последствий, возникающих вследствие прекращения или нарушения их функционирования;

– разработка требований и реализация мер по обеспечению информационной безопасности критически важных объектов информационной и телекоммуникационной инфраструктуры.

Создание единой государственной системы контроля состояния безопасности информационно-телекоммуникационных систем связано с необходимостью проведения организационных мероприятий, направленных на управление контролем над состоянием информационной безопасности, проводимой ведомственными органами контроля, а именно:

– создание единой нормативной базы по проведению контроля состояния информационной безопасности для всех органов и организаций критически важных объектов информационной и телекоммуникационной инфраструктуры;

– учет результатов контроля в единой базе данных органа, уполномоченного в области обеспечения безопасности критически важных объектов информационной и телекоммуникационной инфраструктуры.

Разработка и принятие закона «Об особенностях обеспечения информационной безопасности критически важных объектов информационной и телекоммуникационной инфраструктуры» необходимы, по мнению автора, для реализации государственной политики в области информационной безопасности страны и позволят упорядочить отношения между государственными органами и субъектами информационной и телекоммуникационной инфраструктуры в указанной области. Многие аспекты взаимоотношений государственных органов и субъектов информационной и телекоммуникационной инфраструктуры требуют более детальной проработки. В частности, очевидно, что обеспечение информационной безопасности таких объектов потребует государственной поддержки.

Третья глава диссертации – **«Система конституционных норм и законодательства в сфере правового обеспечения информационной безопасности»,** охватывает два параграфа.

В первом параграфе – «Правовые гарантии обеспечения информационной безопасности в Российской Федерации», исследуются нормативно правовые акты Российской Федерации**.** В Конституции Российской Федерации содержится более 20 норм, связанных с обеспечением информационной безопасности. Конституционные нормы определяют и устанавливают как принципиальную, так и непосредственную основу информационного права в статьях 15, 17, 18, 19, 23, 24, 29, 41 и т. д. Часть из перечисленных конституционных норм регламентирует материально-правовые стандарты в области информационной безопас-

ности. В целях реализации материально-правовых стандартов, Конституция Российской Федерации устанавливает процессуальные гарантии их реализации и механизмы ответственности. Общепризнанными гарантиями являются: признание прав и свобод человека неотчуждаемыми (статья 17), равными (статья 19) и непосредственно действующими (статья 18). Механизмы охраны предусматривают государственную защиту, право каждого на самозащиту всеми не запрещенными законом способами (часть 2 статьи 45), судебную (части 1 и 2 статьи 46) и международно-правовую защиту (часть 3 статьи 46).

В части 4 статьи 29 Конституции закреплено право каждого свободно искать, получать, передавать, производить и распространять информацию любым законным способом. В конституционном порядке закреплены исключения по отношению сведений, составляющих государственную тайну. В конституционном порядке закреплены права граждан на неприкосновенность частной жизни, личную и семейную тайну, тайну переписки, телефонных переговоров, телеграфных и иных сообщений (статья 23). В соответствии со статьей 24 Конституции Российской Федерации, не допускается сбор, хранение и распространение информации о частной жизни лица без его согласия.

Пунктом 2 статьи 24 Конституции установлена обязанность органов государственной власти и местного самоуправления обеспечить для каждого возможность ознакомиться с непосредственно затрагивающими его права и свободы документами и материалами. В Конституции закреплена также обязанность государства официально публиковать нормативные правовые акты, затрагивающие права и обязанности человека и гражданина (часть 3 статьи 15), обстоятельства, создающие их (часть 3 статьи 41).

Среди законов в рассматриваемой области, прежде всего, следует отметить кодифицированные правовые акты: Таможенный кодекс Российской Федерации от 28.05.2003 года № 61-ФЗ, Гражданский кодекс Российской Федерации от 30.11.1994 года № 51-ФЗ (часть первая), от 26.01.1996 года № 14-ФЗ (часть вторая), от 18.12.2006 года №231-ФЗ (часть четвертая), Уголовный кодекс Российской Федерации от 13.06.1996 года № 63-ФЗ, Уголовно-исполнительный кодекс Российской Федерации от 08.01.1997 года № 1-ФЗ, Налоговый кодекс Российской Федерации от 31.01.1998 года № 146-ФЗ (часть первая) и 05.08.2000 года № 117-ФЗ (часть вторая), Трудовой кодекс Российской Федерации от 30.12.2001 № 197-ФЗ и другие.

Многие из кодифицированных актов содержат правовые нормы, которые регулируют различные вопросы информационной безопасности. Например, Гражданский кодекс Российской Федерации 30.11.1994 года № 51-ФЗ (часть первая) статьей 139 определяет понятия служебной и коммерческой тайны, статьей 150 - устанавливает режим защиты личной и семейной тайны. Статьями 160 и 779 регулируются информационные услуги, вопросы электронной подписи.

Важное место среди нормативных правовых актов в области информационной безопасности занимает Уголовный кодекс Российской Федерации. Впервые в российском законодательстве преступлениям в сфере компьютерной информации посвящена отдельная глава (глава 28, статьи 272-274) Уголовного кодекса Российской Федерации. Кроме этого, в Уголовном кодексе Российской Федерации устанавливается ответственность за нарушение неприкосновенности частной жизни (статья 137), тайны переписки (статья 138), ответственность за отказ в предоставлении гражданину информации (статья 140), ответственность за разглашение государственной тайны (статья 283) и другие преступления в данной сфере.

Кодификация, конечно, не первоисточник структуры права. Системность нормативных обобщений получает развитый характер в отдельных специальных нормативных актах. Среди основополагающих актов законодательства об информационной безопасности важное место занимают законы Российской Федерации: от 27.12.1991 года № 2124-I «О средствах массовой информации», от 05.03.1992 года № 2446-I «О безопасности», от 21.07.1993 года № 5485-I «О государственной тайне» и федеральные законы: от 27.07.2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации», от 27.07.2006 года № 152-ФЗ «О персональных данных», от 29.12.1994 года № 77-ФЗ «Об обязательном экземпляре документов», от 06.04.2011 года № 63-ФЗ «Об электронной подписи» и другие. Федеральный закон «Об информации, информационных технологиях и о защите информации» является базовым в информационной сфере. В нем содержатся определения основных понятий.

Федеральными законами могут быть установлены ограничения использования определенных средств защиты информации и осуществления отдельных видов деятельности в области защиты информации. В Законе Российской Федерации «О средствах массовой информации» от 27.12.1991 года № 2124-I регламентированы вопросы о недопусти-

мости злоупотребления свободой массовой информации (статья 4), конфиденциальность информации (статьи 41), обязанность журналиста получать согласие на распространение в СМИ сведений о личной жизни гражданина (статья 49) и другие.

Среди указанных актов в Законе Российской Федерации от 05.03.1992 года № 2446-I «О безопасности» раскрывается понятие безопасности. Под безопасностью понимается состояние защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз. В Законе также рассматриваются жизненно важные интересы личности, общества и государства (статья 1).

Большое значение в рассматриваемой сфере имеет принятый 10.01.2002 года Федеральный закон «Об электронной цифровой подписи». В законе рассматривается значение электронной цифровой подписи. В Законе нашли законодательное закрепление понятий электронного документа и электронной цифровой подписи (ст.3). Хотя данный закон учредил новый правовой институт, однако, он нуждается в существенной переработке в части использования иных аналогов собственноручной подписи, а также в приведении его в соответствие с требованиями международных правовых актов.

Правоотношения в области обеспечения информационной безопасности регулируются нормами Федерального закона Российской Федерации от 21.07.93 года № 5485-I «О государственной тайне». Данный закон регулирует отношения, возникающие в связи с отнесением сведений к государственной тайне, их засекречиванием или рассекречиванием и защитой в интересах обеспечения безопасности государства, полномочия и ответственность государственных органов и их должностных лиц. Также даны определения государственной тайны, допуска к государственной тайне и доступа к сведениям, составляющим государственную тайну.

Порядок доступа к персональным данным граждан устанавливается Федеральным законом «О персональных данных». В законе заложены основные принципы правового регулирования деятельности, связанной с персональными данными. Вводится ответственность за нарушение их конфиденциальности, а также режим деятельности, связанной с обработкой и представлением персональных данных.

Законодательством вводятся также и понятия «банковская тайна», «тайна связи», «служебная и коммерческая тайна», «налоговая тайна» и т.д. Например, в части первой Гражданского кодекса Российской Федерации установлены такие правовые режимы информации, как служебная и коммерческая тайна (статья 139), а также личная и семейная тайна (статья 150). В Законе «О почтовой связи» установлено понятие «тайна связи» и определяется круг лиц, допущенных к ней и обеспечивающих ее соблюдение (статья 2).

Статья 139 Гражданского кодекса Российской Федерации дает определение понятию «служебная или коммерческая тайны». Отмечается, что информация составляет служебную или коммерческую тайну в случае, когда информация имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к ней нет свободного доступа на законном основании, и обладатель информации принимает меры к охране ее конфиденциальности.

В соответствии со статьей 313 Налогового кодекса Российской Федерации содержание данных налогового учета является налоговой тайной. Нормы, посвященные соблюдению конфиденциальности информации и защите тайн, содержатся также в законодательстве о банках. Статьей 26 Федерального закона «О банках и банковской деятельности» установлено, что кредитные организации гарантируют тайну об операциях, о счетах и вкладах своих клиентов и корреспондентов.

Вопросам защиты персональных данных посвящена статья 85 Трудового кодекса Российской Федерации от 30.12.2001 № 197-ФЗ. Указанная статья содержит определение персональных данных работника. Под персональными данными понимается информация, которая необходима работодателю в связи с трудовыми отношениями и касающаяся конкретного работника.

Среди правовых актов следующего уровня, к которому относятся указы Президента Российской Федерации, можно выделить основные блоки нормативных правовых актов: касающиеся защиты информации (в том числе, технической защиты); по вопросам доступа граждан к информации; устанавливающие компетенцию органов государственной власти в сфере защиты информации; касающиеся международного сотрудничества в данной сфере, включая государства-члены СНГ.

Наиболее важной при рассмотрении вопроса о совершенствовании правового регулирования в данном перечне представляется проблема категории персональных данных. Важнейшее значение в развитии информационного законодательства в сфере обеспечения информационной безопасности имеет приведение законодательства в соответствие с ратифицированной Российской Федерацией Европейской

Конвенцией о защите физических лиц при автоматизированной обработке персональных данных.

К следующему блоку можно отнести указы Президента Российской Федерации. В качестве следующего уровня системы среди подзаконных актов в этой области необходимо отметить постановления Правительства Российской Федерации. Определение структуры системы законодательства в области информационной безопасности «по горизонтали» позволяет классифицировать правовые нормы, касающиеся вопросов обеспечения информационной безопасности, по отраслям законодательства, в частности, на примере норм, касающихся ответственности за нарушение законодательства в указанной сфере.

Нельзя рассматривать информационную безопасность отдельно от национальной безопасности. В соответствии с концепцией национальной безопасности, субъекты Российской Федерации обладают огромными информационными ресурсами, и они формируют единое правовое пространство. В большинстве субъектов Российской Федерации приняты нормативные правовые акты в соответствии с федеральным нормативном актом, в которых урегулированы вопросы информационной безопасности.

Анализ федерального законодательства позволяет сделать вывод, что в систему законодательства в области обеспечения информационной безопасности включаются все отраслевые нормы законодательства и структура во многом определяется основными направлениями правового регулирования таких вопросов как защита информационных прав и свобод личности; защита информационных систем от неправомерного воздействия; защита интересов общества от воздействия различных угроз. Анализ законодательства позволяет сделать также вывод о необходимости упорядочения законодательства в области информационной безопасности определения принципов реализации государственной политики. Действующее законодательство в области обеспечения информационной безопасности в Российской Федерации характеризуется:

– противоречивостью;

– отсутствием системности;

– декларативностью (например, в законодательстве перечисляются более 40 видов тайн, а в соответствующих кодексах упоминается всего пять, за разглашение которых предусмотрена ответственность);

– отсутствием регулирования ряда ключевых вопросов.

Чтобы устранить указанные негативные тенденции, представляется целесообразным совершенствование законодательства, а именно, определение предметной области законодательства в сфере обеспечения информационной безопасности.

Во втором параграфе третьей главы – «**Системный анализ правового обеспечения информационной безопасности в Азербайджанской Республике»,** проведен системный анализ правового обеспечения информационной безопасности в Азербайджанской Республике. Здесь указывается, что системный анализ правового обеспечения информационной безопасности необходимо начать с конституционно-правовых норм.

Конституция Азербайджанской Республики охватила почти все международно-признанные права и свободы человека. В настоящее время, когда Азербайджанская Республика вступила на путь демократического развития, нормы международного права уже не являются для гражданина Азербайджана просто отвлеченным понятием, а должны рассматриваться как прямые гарантии прав граждан. Оптимальный путь реализации норм международного права - это принятие внутригосударственных законов, соответствующих этим нормам и конкретизирующие их. Одним из средств по приведению или регулированию соответствующих отношений в соответствии с международно-правовыми нормами является законодательное закрепление нормы о «международный деятельности в сфере информации» (Закон Азербайджанской Республики «Об информации, информатизации защите информаций», ст.21), об источнике законодательства (Закон Азербайджанской Республики «О персональных данных», ст.3). Согласно статье 3 Закона «Об электронной торговле» законодательство Азербайджанской Республики об электронной торговле состоит из Конституции Азербайджанской Республики, Гражданского кодекса Азербайджанской Республики, Законов Азербайджанской Республики «Об электронной подписи и электронном документе», «Об электронной торговле» и других нормативно-правовых актов, а также международных соглашений, стороной которых является Азербайджанская Республика.

В Конституции закреплено право на информацию и также механизмы реализации этого права. Статья 50 гарантирует каждому право получать и распространять информацию. Специальным законодательным актом в области обеспечения информационной безопасности является принятый 3 апреля 1998 года Закон «Об информации, информатизации и защите информации». В вопросе о получении информации существенное

значение имеет Закон Азербайджанской Республики «О получении информации», принятый 30 сентября 2005 года.

По видам получения информация подразделяется на открытую для общего использования информацию и информацию, получение которой ограничено. Информация, получение которой ограничено законом, является секретной или тайной. Ограниченная для пользования информация определяется в различных законодательных актах. Соответственно можно выделить следующие виды информации: информация, составляющая государственную, врачебную, нотариальную, адвокатскую, служебную, коммерческую, следственную тайну. С целью обеспечения безопасности Азербайджанской Республики отнесение информации к государственной тайне, ее защита и пользование определяется Законом Азербайджанской Республики «О государственной тайне». Правовой основной института государственной тайны является ст. 50 Конституции, также Законы «О безопасности», «О государственной тайне», «Об информации, информатизации и защите информации» и др. Должностные лица и граждане, нарушающие законодательство Азербайджанской Республики о государственной тайне, несут уголовную, административную, гражданско-правовую или дисциплинарную ответственность. Информация, составляющая врачебную тайну, регулируется согласно Закону Азербайджанской Республики «О защите здоровья населения». В соответствии со статьей 13 Семейного кодекса Азербайджанской Республики результаты медосмотра лиц, вступающих в брак, относятся к врачебной тайне. Информация, составляющая врачебную тайну, может быть использована с разрешения гражданина или его законного представителя с целью проведения лечения пациента, проведения научных исследований, опубликования в научной литературе и в других случаях. Нотариальная тайна, и связанные с ней вопросы, регулируются Законом Азербайджанской Республики «О нотариате». В соответствии с законодательством, нотариальную тайну составляют сведения, справки и документы о проведении нотариальной деятельности, в том числе, ставшие известными нотариусу, в связи с осуществлением им профессиональной деятельности, факты и сведения о личной и семейной жизни граждан. Хранение нотариальной тайны – обязанность нотариуса.

Коммерческая тайна регулируется Законом Азербайджанской Республики «О коммерческой тайне», Налоговым кодексом Азербайджанской Республики и другими законодательными актами. В соответствии с Законом о коммерческой тайне таковой считаются сведения о производстве, технологии, управлении, финансах и другие, разглашение которых без разрешения собственника могут нанести ущерб.

Информация о личности собирается на законных основаниях. Статьей 130 Семейного кодекса Азербайджанской Республики предусмотрена охрана тайны усыновления. Соответственно распространение сведений без разрешения усыновителей (в случае их смерти без разрешения органов опекунства и попечительства) запрещается. Так, информация о религиозной принадлежности дается лицом добровольно. Запрещается сбор информации обманным способом и с применением насилия или угрозы таковой.

Тайна следствия – к ней относят сведения, получаемые в ходе предварительного следствия и судебного расследования, распространение которых может нарушить интересы сторон процесса, а также права и интересы других участников. В соответствии со статьей 222 Уголовно-Процессуального кодекса Азербайджанской Республики такая информация может быть использована с условием соблюдения интересов и прав сторон.

Важным является законодательное регулирование составов компьютерных преступлений (т.е. перечень признаков, характеризующих общественно опасное деяние как конкретное преступление) приведенных в главе 30 Уголовного кодекса Азербайджанской Республики, которая называется «Киберпреступления» и содержит пять статьей: «Неправомерный доступ к компьютерной системе» (ст. 271), «Неправомерное завладение компьютерной информацией» (ст. 272), «Неправомерное вмешательство в компьютерную систему или компьютерную информацию» (ст. 273), «Оборот средств, изготовленных для совершения киберпреступлений» (ст. 273-1) и «Фальсификация компьютерных данных» (ст. 273-2).

Статья 271 Уголовного кодекса Азербайджанской Республики предусматривает уголовную ответственность за преднамеренный вход в компьютерную систему или ее какую-либо часть без права доступа в эту систему или ее какую-либо часть с нарушением мер защиты, либо с целью завладения хранящейся в ней компьютерной информацией или с иной личной целью. В статье 272 УК устанавливается ответственность за преднамеренное завладение с использованием технических средств компьютерной информацией, не предусмотренной для общего пользования, передаваемой компьютерной системе, из компьютерной системы или внутри этой системы, в том числе электромагнитным излучением от компьютерных систем, являющихся носителем такой компьютерной инфор-

мации, лицом, не имеющим права на это, а в статье 273 Уголовного кодекса Азербайджанской Республики – за преднамеренное повреждение, уничтожение, порча, изменение или блокирование компьютерной информации, совершенное лицом, не имеющим право на это, с причинением значительного ущерба. Довольно интересен состав преступления в ст.273-1, предусматривающей ответственность за оборот средств, изготовленных для совершения киберпреступлений. Несанкционированное, преднамеренное введение, изменение, уничтожение или блокирование компьютерных данных с целью выдать фальсифицированные компьютерные данные за аутентичные (действительные) компьютерные данные или использовать их, если эти деяния повлекли нарушение аутентичности (действительности) первичных компьютерных данных влечет уголовную ответственность по ст.273-2 Уголовного кодекса. Всего же в главе 30 Уголовного кодекса Азербайджанской Республики устанавливается уголовная ответственность за 15 составов преступлений, которые являются преступлениями, не представляющими большой общественной опасности, или менее тяжкими преступлениями.

Четвертая глава диссертации – **«Правовые вопросы построения информационного общества»** состоит из трех параграфов.

В первом параграфе - **«Нормативные основы развития информационного общества»,** исследуются нормативные основы информационного общества.

Концепция социально-экономического развития Российской Федерации на период до 2020 года определяет цели государственной политики в области развития информационных технологий. 20 октября 2010 года распоряжением Правительства Российской Федерации № 1815-р утверждена Государственная программа Российской Федерации «Информационное общество (2011 – 2020 годы)» (впоследствии принята совершенно новая редакция – прим. автора), в которой важное место уделяется развитию и внедрению механизмов «электронного» государства.

Основными задачами создания информационного общества являются создание юридических основ информационного общества, развитие прав граждан на получение информации, ее распространение и использование, формирование прозрачного государственного аппарата и аппарата местного самоуправления, электронного государства, электронной торговли, создание экономики, устойчивой к конкуренции, обеспечение информационной безопасности, интеграция в глобальное информационное пространство и другие необходимые задачи.

За период, прошедший со дня принятия Национальной стратегии, правительством Азербайджанской Республики был осуществлен ряд комплексных мер и принят целый ряд нормативно-правовых актов. Одним из таких актов является Закон «Об электронной торговле», который способствует осуществлению операций купли-продажи, оказанию разного типа торговых услуг, заключению договоров электронным способом в сети, а также развитию экономических отношений между странами в глобализирующем мире. В соответствующие нормативные акты Азербайджанской Республики были имплементированы принципы электронной торговли 1996 года, принятые Комиссией ООН по Международному торговому праву. Наиболее полными нормами, регулирующими данные отношения, обладают принятые Национальным Банком Азербайджанской Республики 2 февраля 2001 года Правила организации расчетов между кредитными организациями. При Национальном Банке начала действовать Межбанковская национальная расчетная система в режиме реального времени AZIPS, члены которого зарегистрированы в S.W.I.F.T., являются членами группы AZM, и работают в режиме У-СОРУ. До этого нормативно-правового акта возможность применения электронного документа отражалась в Гражданском кодексе Азербайджанской Республики, вступившим в силу с 1 сентября 2000 года. Принятый 25 июня 2002 года Закон Азербайджанской Республики «О телерадиовещании» тоже имеет нормы по использованию интернета. Закон «О телекоммуникации» отображает в себе телекоммуникационные сети и операторов, отношения между ними, а также механизм управления в этой области. Указом Президента Азербайджанской Республики от 3 сентября 2000 года при Центральной Избирательной Комиссии Азербайджанской Республики был создан информационный центр «Seçkilər» («Выборы»).

Таким образом, создание информационного общества рассматривается как платформа для решения задач более высокого уровня - модернизации экономики и общественных отношений, обеспечения конституционных прав граждан и высвобождения ресурсов для личностного развития.

Второй параграф четвертой главы - **«Основные направления обеспечения правового регулирования информационной безопасности информационного общества»,** посвящен правовым элементам информационного общества, формированию электронного правительства. Процесс постоянного развития и распространения в глобальном масштабе информационно-коммуникационных технологий, имеющий

краткосрочные и долгосрочные последствия, можно назвать процессом «глобальной информатизации». Информатизация определяется как новый этап в развитии производительных сил, при котором обмен информацией, ее оперативная обработка и эффективное применение являются определяющими условиями всестороннего развития общества.

В Окинавской хартии глобального информационного общества, принятой странами «большой восьмерки» 22 июля 2000 года, отмечено, что «информационно-коммуникационные технологии являются одним из наиболее важных факторов, влияющих на формирование общества XXI века». Концепция информационного общества сегодня становится составной частью, реально проводимой многими государствами и межгосударственными объединениями, информационной политики. Для формирования информационного общества необходимо практическое осуществление целого ряда проектов. Среди них важнейшими являются проекты по созданию концепций «электронное государство» и «электронное правительство». Электронное государство - способ осуществления информационных аспектов государственной деятельности, основанный на использовании ИКТ-систем. Электронное государство подразумевает поддержку при помощи ИКТ деятельности как исполнительной власти («электронное правительство»), так и парламентских («электронный парламент») и судебных органов («электронное правосудие»).

Таким образом, делается акцент на том, что электронное правительство не как частичное технологическое решение, а как концепция осуществления управления государством, является необходимым элементом масштабного информационного преобразования общества. Изменение нормативно-правовой базы, образовательных приоритетов, принципов формирования и расходования бюджета, экологических ориентиров, перераспределение зон приоритетной компетенции государственных и общественных структур, перенесение акцентов в экономике, обновление и расширение ценностных приоритетов общества – все это вместе со многими другими компонентами жизнедеятельности общества является основой для государственного управления, для создания и функционирования электронного правительства.

Проект «Национальная Инициатива Сети Э-Управления» играет роль платформы для развития электронного управления в Азербайджане. Подписание проекта 14 июля 2004 года, в первую очередь, было вызвано обязательствами, взятыми Азербайджанкой Республикой с целью развития электронного управления, а также большой поддержкой, оказываемой Программой Развития ООН развитию общей ИКТ инфраструктуры. В отдельности, Э-Управление считается основным компонентом в реализации девиза «Превратим черное золото в золото для человека», основанного на вложении нефтяных и газовых прибылей в развитие экономики, науки и социальной инфраструктуры. Этот проект является успешным продолжением Проекта Стратегии Национальной Информации и Коммуникации (NICTS-1), развивающего Национальную Стратегию ИКТ Азербайджана. Помимо оказания общественных услуг, электронное управление предоставляет возможность для развития демократических процессов, создавая возможность активного участия граждан в увеличении прозрачности в правительстве, уменьшении коррупции в исполнительных и законодательных органах.

В данном параграфе рассматривается также развитие направлений правового регулирования информационной безопасности. Отмечается, что при построении информационного общества важнейшими целями административной реформы являются повышение качества и доступности государственных услуг. Представляется, что основные мероприятия административной реформы, касающиеся напрямую рассматриваемой темы, должны быть реализованы по следующим направлениям:

– разработка стандартов массовых общественно значимых государственных услуг, предоставляемых органами исполнительной власти;

– разработка и принятие нормативных актов, упраздняющих дублирующие функции, осуществляемые органами исполнительной власти.

Работа по этим направлениям должна носить системный характер и осуществляться на основе взаимодействия государственных органов и органов местного самоуправления при оказании государственных услуг гражданам и организациям.

Следует отметить, что в настоящее время отсутствует необходимая нормативно-правовая база для стандартизации услуг, предоставляемых органами исполнительной власти, включая услуги общего экономического характера (они находятся в стадии формирования), а также неэффективна существующая система обратной связи с пользователями государственных услуг. В рамках административной реформы важно решить вопрос влияния гражданского общества (граждан, организаций, делового сообщества) на подготовку и принятие затрагивающих их права и законные интересы решений органов исполнительной власти и принятие соответствующих правовых актов. В связи с этим, автор полагает необходимой разработку методических основ и

систем мониторинга процессов управления по результатам качества предоставления государственных услуг, результативности ведомственных и региональных антикоррупционных программ, проведения закупок для государственных нужд, информационной открытости органов исполнительной власти и органов местного самоуправления, развития гражданского общества и участия его представителей в процессе подготовки и принятии государственными органами решений.

Таким образом, в целях реализации указанных мероприятий необходим переход на применение в статистической практике новых национальных классификаторов, гармонизированных с международными аналогами и открытость органов государственной власти.

По мнению автора, создание самостоятельных систем мониторинга по каждому из перечисленных направлений, связанных с созданием и внедрением отдельных систем мониторинга закупок для публичных нужд, информационной открытостью органов государственной власти и органов местного самоуправления, развитием гражданского общества и участием его представителей в подготовке и принятии решений, является необходимым условием успешной реализации административной реформы

В третьем параграфе четвертой главы – «**Основные направления внедрения электронного документооборота в период развития информационного общества»,** раскрываются направления развития информационного общества. Направления развития информационного общества можно рассмотреть на примере трех основных, так называемых, модулей правовой информатизации: модуль «электронный документооборот»; модуль развития технологий электронного правительства в судебных органах; модуль «электронных закупок».

Базовые нормы законодательства, оказывающие непосредственное воздействие на использование электронного документооборота, содержатся в различных нормативных актах: «Об информации, информационных технологиях и защите информации»; Гражданском кодексе, предусматривающем возможность заключения договора путем обмена документами посредством «...телеграфной, телетайпной, телефонной, электронной или иной связи», а также «использования электронной цифровой подписи либо иного аналога собственноручной подписи случаях и порядке, предусмотренных законодательными актами или соглашением сторон»; «Об электронной цифровой подписи», определяющем условия признания равнозначности электронной цифровой подпи-

си и собственноручной подписи, а также регламентирующем применение при совершении сделок электронной цифровой подписи.

Органы законодательной власти широко применяют систему электронного документооборота (СЭД) в своей деятельности и после завершения работ по созданию «электронного парламента» смогут и на региональном уровне полностью перейти на электронный документооборот. При внедрении СЭД важно довести до сознания людей новую трактовку автоматизации: внедрение системы будет означать не сокращение потребности в персонале, а возможность выполнения работы на другом качественном уровне.

Электронный документооборот применяется и в сфере налоговых отношений. Вступившие в силу поправки в Налоговый кодекс Азербайджанской Республики предусматривают, что налоговая декларация может быть направлена налогоплательщиком в налоговый орган по телекоммуникационным каналам связи. Можно сказать, что развитие системы электронного документооборота позволяет утверждать, что уже в обозримом будущем каждый гражданин или организация смогут направить или получить любой требуемый документ из любого государственного органа в электронном виде.

Компьютеризация судов является стратегическим направлением повышения оперативности судопроизводства. Активное создание сайтов судебных органов в интернете позволяет с оптимизмом смотреть на развитие принципа гласности судебного процесса. Так, не все желающие присутствовать на процессе и тем самым реализовать свое законное право, могут это желание осуществить. В число причин таких вынужденных неявок можно отнести инвалидность, необходимость присутствия на работе, в доме, большие расстояния, а также много других причин.

Технологии электронной подписи, а также иные защитные программы служили бы гарантией информационной безопасности судебного процесса. Информатизация судебной системы позволила бы решить и проблему протоколирования судебного процесса. Таким образом, требует решения вопрос, и это особенно важно для судебной системы, какие именно иные аналоги собственноручной подписи могут использоваться в официальном электронном документообороте. Посредством электронной связи могут быть направлены судебные извещения, повестки и акты. Однако в этом случае возникает проблема определения места и времени отправления и получения электронных сообщений, а также подтверждения

получения документов той стороной процесса, которой они направлены. В законодательстве эти вопросы не урегулированы.

Анализ состояния организационно-правового обеспечения в информационной сфере, проведенный в рамках настоящего исследования, позволяет сделать вывод о том, что теоретические и методологические основы государственного регулирования в информационной сфере целесообразно сосредоточить в едином документе концептуального характера, определяющем развитие информационного законодательства.

Пятая глава диссертации – **«Обеспечение информационной безопасности в сети интернет»,** состоит из двух параграфов.

В первом параграфе - **«История и современное состояние функционирования сети Интернет»,** исследуются нормативные вопросы функционирования сети Интернет. Internet = inter + net – объединение сетей – всемирная компьютерная сеть, объединяющая миллионы компьютеров в единую информационную систему. Интернет возник как воплощение двух идей — глобального хранилища информации и универсального средства ее распространения.

Можно сделать вывод, что Интернет является не единой сетью, а только общей системой взаимодействия множества сетей. Его децентрализованный характер позволяет объединять в одной системе самые разные элементы. Существование отдельного элемента сети Интернет не обязательно связано только с его включением в эту глобальную информационную систему, поскольку последняя объединяет в себе различные по размерам и построению как целые сети (от нескольких компьютеров до многих десятков тысяч), так и отдельные компьютеры. Для передачи данных могут использоваться самые разные способы связи – от телефонных и выделенных линий до спутниковых каналов и даже линий электропередач. При этом назначение каждой сети, принципы ее организации и внутреннего взаимодействия, а также размеры устанавливаются владельцем сети и не предопределяются ее вхождением в Интернет. Подключение как отдельного компьютера, так и локальных компьютерных сетей к глобальной Сети осуществляется лишь в той степени, в какой это требуется владельцу такой локальной сети, отвечает его интересам и осуществляется на добровольных началах. Владелец каждого элемента сети Интернет может ограничить его взаимодействие с глобальной Сетью фрагментарным подключением для передачи данных или получения определенной информации, а может практически полностью интегрировать свою локальную сеть в Интернет.

При регистрации сети в интернете, ей выделяется определенный диапазон адресов, которые могут использоваться в этой сети. Например, провайдер коммутируемого доступа, то есть компания, которая предоставляет доступ в интернет по телефону. При подключении дозвонившегося и указавшего верный логин и пароль абонента, ему присваивают свободный IP-адрес, который после отключения может быть передан другому абоненту. Адреса используются сетевыми устройствами-маршрутизаторами для передачи сообщений в нужном направлении. Но обычный пользователь ищет не какой-то конкретный компьютер, а определенную информацию. Совокупность файлов образует сайт. Сайт принадлежит какому-либо лицу или организации и имеет уникальный адрес. Он ведет на главную страницу сайта, с которой открывается доступ к другим страницам. Для удобства составления и запоминания адресов сайтов совместно с IP-адресацией действует Система Доменных Имен (DNS — Domain Name System, domain — зона, владение). Все его информационное пространство разделено на зоны первого уровня по принадлежности к стране (.RU - Россия, .UC- Украина, .AZ - Азербайджан) или по профилю ресурса (.com - коммерческие организации, .edu - образовательные учреждения). Следует сказать, что доменный адрес не связан напрямую с физическим расположением ресурса. Сайт ... .az может размещаться на компьютере, находящемся, например, в Британии. Регистрацией доменов первого уровня занимается международная организация ICAAN (Internet Corporation for Assigned Names), второго — соответствующие национальные организации. В России это RU-Center (Региональный сетевой информационный центр, РСИЦ). В Азербайджанской Республике интернет функционирует с 90-х годов XX в., точнее, с 1991 года с применением электронно-почтовой службы. В 1991 году НАН Азербайджана было реализовано присоединение к интернету.

Во втором параграфе пятой главы - **«Обеспечение информационной безопасности и правовое регулирование доступа к информации»,** рассматриваются проблемы доступа к информации в глобальной сети Интернет. Защита информации в глобальной сети Интернет имеет свою специфику, отличающую ее от проблемы защиты информации в локальных сетях. Важнейшей отличительной особенностью задачи защиты информации в глобальной сети является тот факт, что защита информации возлагается на программно-аппаратные средства.

Другой особенностью проблемы является огромная скорость развития в интернете программного обеспечения и технологий. Все-

мирная сеть позволяет сотрудникам компаний мгновенно обмениваться информацией, не покидая своего рабочего места. Однако с подключением к интернету перед организациями встает проблема защиты корпоративных ресурсов от различных видов угроз. При использовании интернета компании должны быть готовы к следующим видам угроз: атаки на корпоративную сеть. Традиционные средства защиты, такие как межсетевые экраны и маршрутизаторы, обеспечивают контроль доступа в корпоративную сеть извне: атаки на web-портал и интернет-магазин. Здесь на первое место выступает защита доступа к системе управления контентом, базе данных, системы электронных платежей, своевременное обнаружение и устранение уязвимостей в программном обеспечении серверов; перехват незашифрованного трафика через проводные и беспроводные каналы. Эта угроза относится ко всем интернет-сервисам, используемым в организации. В проводных сетях данные могут быть перехвачены путем получения физического доступа к среде передачи. Широкое распространение получили и несанкционированные беспроводные сети с бесплатными точками доступа. Когда пользователь подключается к ложной точке доступа, хакер может сделать с его компьютером все, что угодно, причем такую атаку обнаружить зачастую невозможно. Зараженная система ничего не подозревающего сотрудника становится «входной дверью» в корпоративную сеть. Более того, злоумышленники могут получить доступ к компьютеру пользователя, даже если он не подключен к Wi-Fi сети. Достаточно того, что устройство беспроводной связи в компьютере пользователя настроено по умолчанию, включено и занято поиском сети. Полученная любым из этих способов информация о корпоративной сети, в том числе логины и пароли сотрудников, помогают злоумышленникам провести успешную атаку. При построении информационного общества проблемы правового обеспечения доступа к информации имеют практически первостепенное значение.

Как граждане, так и организации, имеют право на получение от государственных органов, органов местного самоуправления, их должностных лиц информации в порядке, установленном законодательством. Государственные органы и органы местного самоуправления обязаны обеспечивать доступ к информации о своей деятельности в соответствии с законами и нормативными правовыми актами органов местного самоуправления. Важным является вопрос о доступе к информации представителей средств массовой информации, которые

имеют право ознакомиться с записями и снять копии с них, исключая записи закрытых мероприятий.

К проблемам законодательства о доступе к информации нужно отнести и недостаточную определенность правового режима информации ограниченного доступа, вообще, и имеющейся в распоряжении государственных органов, в частности. Одной из ключевых проблем функционирования системы исполнительной власти является информационная закрытость органов исполнительной власти и органов местного самоуправления, а также отсутствие обратной связи с гражданами и организациями.

Среди нерешенных проблем в сфере обеспечения права на доступ к информации отмечается отсутствие единого нормативного правового акта, закрепляющего основные права граждан и организаций в области доступа к информации, основные принципы предоставления информации и механизм реализации права на доступ к информации; четкой регламентации задач и функций органов государственной власти при формировании открытых государственных информационных ресурсов и обеспечения доступа к ним граждан и организаций; а также единого порядка информационного обмена органов государственной власти с гражданами и организациями посредством использования информационных систем общего пользования.

В заключение диссертационной работы подводятся итоги проделанной работы, обобщаются основные положения и выводы, которые, по мнению автора, должны усовершенствовать теоретические и конституционные основы правового обеспечения информационной безопасности при построении информационного общества Азербайджанской Республики и Российской Федерации.

По теме диссертационного исследования автором опубликованы следующие научные работы:

1. Rusiya dövlətinin informasiya texnologiyaları təhlükəsizliyinin hüquqi təminatı. Monoqrafiya. Bakı, Qanun, 2010, 328 s.

2. Основы информационного права. Учебное пособие. Баку, Ганун, 2010, 456 с.

3. Административное право. Учебник. Баку, Ганун, 2010, 568 с.

4. Конституция Азербайджанской Республики и основы права. Учебник. Баку, Ганун, 2010, 464 с.

5. Сравнительный анализ правового обеспечения информационной безопасности при построении информационного общества в

Российской Федерации и Азербайджанской Республике. Монография. Москва, 2012, 424 с.

6. Rusiyada informasiya təhlükəsizliyinin təşkilati-hüquqi təminatı. Monoqrafiya. Bakı, Qanun, 2014, 312 s.

7. Законодательство Азербайджанской Республики о государственной тайне. Пробелы в Российском законодательстве, Москва, 2012, №2, с. 241-244.

8. Основные направления развития информационного общества. Образование наука. Научные кадры, Москва, 2012, №2, с. 36-39.

9. Зарубежный опыт правового регулирования обеспечения информационной безопасности. Политика и общество, 2012, Москва, №2(86), с. 45-48.

10. Системный анализ правового обеспечения информационной безопасности в Российской Федерации. Национальная безопасность, Москва, 2012, №2(19), с. 56-59.

11. Преподавание дисциплины «Правовое обеспечение информационной безопасности» в Российской правовой академии. Правовой мониторинг, Москва, 2010, №11, с. 4-7.

12. Правовое регулирование обеспечения доступа к информации. Право и политика, Москва, 2012, №2(146), с. 305-307.

13. Методология организации процессов регулирования информационной безопасности. Пробелы в Российском законодательстве, Москва, 2012, №1, с. 263-265.

14. Институт тайны и нормы уголовного права при регулировании информационных отношений в Азербайджанской Республики. «Черные дыры» в Российском законодательстве, Москва, 2012, №1, с. 132-135.

15. Законодательство Азербайджанской Республики о коммерческой тайне. Теория и практика общественного развития, Москва, 2012, №2, с. 359-361.

16. Международное правовое регулирование в сфере обеспечения информационной безопасности. Закон и право, Москва, 2012, №3, с. 104-106.

17. Правовое регулирование порядка использования информационных технологий в формировании основ информационного общества в Российской Федерации. Закон и право, Москва, 2012, №8, с. 107-108.

18. Взаимодействие информации и права как структурных элементов информационного общества. Закон и право, Москва, 2012, №9, с. 95-96.

19. Конституционные и законодательные нормы регулирования информационных отношений в Азербайджанской Республике. Этносоциум и межнациональная культура, Москва, 2012, №1(43), с. 159-166.

20. Системный анализ правового обеспечения информационной безопасности в Азербайджанской Республике. Управление мегаполисом, Москва, 2012, №2, с.78-84.

21. Сравнительно-правовой анализ информационного законодательства Российской Федерации и Азербайджанской Республики. Первая международная научно-практическая конференция «Направления и этапы развития информационного права». Сборник докладов. Первая часть. Москва, 2009, с. 23-25.

22. Виды правонарушений в сети Интернет. Beynəlxalq hüquq və inteqrasiya problemləri (elmi-analitik və praktiki jurnal), Bakı, 2013, №4 (36), s. 165-184.

23. Правовое регулирование доступа к информации. Beynəlxalq hüquq və inteqrasiya problemləri (elmi-analitik və praktiki jurnal), Bakı, 2014, №3 (39), s. 191-198.

24. История и современное состояние функционирования сети Интернет. Beynəlxalq hüquq və inteqrasiya problemləri (elmi-analitik və praktiki jurnal), Bakı, 2014, №4 (40), s. 214-219.

25. Современные угрозы информационной безопасности. Naxçıvan Dövlət Universiteti, Elmi əsərlər, İctimai elmlər seriyası, Naxçıvan, 2015, №2(67), s. 119-127.

26. Обеспечение информационной безопасности в сети Интернет. Milli Aviasiya Akademiyası, Elmi məcmuələr, Bakı, 2015, Cild 17, №1, s. 138-146.

27. Понятие информационной безопасности и ее роль в развитии информационного общества. Nəqliyyat hüququ (elmi-nəzəri, təcrübi jurnal), Bakı, 2015, №1, s. 101-110.

28. Основные направления внедрения электронного документооборота в период развития информационного общества. Nəqliyyat hüququ (elmi-nəzəri, təcrübi jurnal), Bakı, 2015, №2, s. 110-122.

29. Стратегия и программы развития информационного общества. Odlar Yurdu Universitetinin elmi və pedaqoji xəbərləri. Humanitar elmlər seriyası, 2015, №42, s. 158-167.

30. Развитие направлений правового регулирования информационной безопасности. Право и политология, Кишинев, 2015, №30 (июнь), с. 23-29.

31. Развитие направлений правового регулирования информационной безопасности критических важных объектов. Закон и жизнь, Кишинев, 2015, №5 (279), с. 41-50.

32. Международные механизмы борьбы с киберпреступностью. Матеріали V Міжнародної науково-практичної конференції - Юридична наука і практика: виклики часу. Київ, 2015, том III, с. 63-67, с. 207-210.

33. İnformasiya təhlükəsizliyi sahəsində mühüm beynəlxalq normalar. Beynəlxalq hüquq və inteqrasiya problemləri (elmi-analitik və praktiki jurnal), Bakı, 2015, №4 (40), s. 34-41/

34. Обеспечение право на информацию: международные стандарты и законодательство Азербайджанской Республики. Nəqliyyat hüququ (elmi-nəzəri, təcrübi jurnal), Bakı, 2015, №3, s. 94-103.

35. Особенности информационных правоотношений в период развития информационного общества. Bakı Universitetinin xəbərləri, Sosial-siyasi elmlər seriyası, 2014, №3, s. 14-27.

36. Теоретические и конституционные основы правового обеспечения информационной безопасности в Азербайджанской Республике и Российской Федерации: сравнительный анализ. Azərbaycan xalqının Ümummilli lideri Heydər Əliyevin anadan olmasının 92-ci ildönümünə həsr olunmuş "Heydər Əliyevin Azərbaycan Respublikasının hüquq elminin və təhsilinin inkişafında rolu" mövzusunda beynəlxalq elmi-praktiki konfransın materialları. Bakı, I cild, 2015, s. c. 21-26.

37. Qloballaşma şəraitində informasiya təhlükəsizliyi sahəsində beynəlxalq əməkdaşlığın bəzi aspektləri. Nəqliyyat hüququ (elmi-nəzəri, təcrübi jurnal), Bakı, 2016, №1, s.204 (1)- 204(8).

38. Право на информацию в законодательстве Азербайджанской Республики. The Computer Law & Security Review (в печати - на английском языке).

XÜLASƏ

Ramil Mahir oğlu Aslanovun 5614.01 – "İnzibati hüquq; maliyyə hüququ; informasiya hüququ" ixtisası üzrə hüquq üzrə elmlər doktoru elmi dərəcəsi almaq üçün təqdim etdiyi "Azərbaycan Respublikası və Rusiya Federasiyasında informasiya cəmiyyəti quruculuğunda informasiya təhlükəsizliyinin hüquqi təminatının nəzəri və konstitusiya əsasları" mövzusunda doktorluq dissertasiya işi müstəqil, yaradıcı və tamamlanmış tədqiqat əsəri olub özündə tamamilə yeni elmi müddəaları əks etdirməklə Azərbaycan Respublikası və Rusiya Federasiyasının hüquq elminin qarşılıqlı aktual problemlərindən biri olan informasiya cəmiyyəti quruculuğunda informasiya təhlükəsizliyinin hüquqi təminatı məsələlərinin geniş təhlilinə həsr olunmuşdur. Dissertasiya işi informasiya təhlükəsizliyinin təmin edilməsi sahəsində geniş universal, regional və ikitərəfli beynəlxalq müqavilə praktikasının, Azərbaycan Respublikası və Rusiya Federasiyası da daxil olmaqla müxtəlif dövlətlərin milli qanunvericiliklərinin və hüquq ədəbiyyatında mövcud fikir müxtəlifliyinin müqayisəli analizi əsasında formalaşdırılmaqla giriş, beş fəsil, nəticə və istifadə olunmuş ədəbiyyat siyahısından ibarətdir.

Girişdə tədqiqat mövzusunun aktuallığı əsaslandırılır, onun işlənilmə dərəcəsi, elmi yeniliyi, müdafiəyə təqdim edilən yeni elmi müddəalar, məqsəd və vəzifələr, tədqiqatın nəzəri və praktiki əhəmiyyəti göstərilir.

Üç yarımfəsildən ibarət olan və "İnformasiya sahəsində təhlükələr və informasiya təhlükəsizliyinin hüquqi təminatının nəzəri əsasları" adlanan dissertasiya işinin I fəslində informasiya təhlükəsizliyinə müasir təhlükələr və onların aradan qaldırılması yolları, informasiya təhlükəsizliyinin anlayışı və onun informasiya cəmiyyətinin inkişafında rolu, informasiya təhlükəsizliyinin hüquqi təminatının metodoloji problemləri kimi mühüm və aktual məsələlər təhlil edilir.

Dissertasiya işinin II fəsli "İnformasiya cəmiyyəti quruculuğunda informasiya təhlükəsizliyinin hüquqi təminatının metodları" adlanır və üç yarımfəsildən ibarətdir. Bu fəsildə informasiya təhlükəsizliyinin təminatı sahəsində beynəlxalq-hüquqi tənzimetmə, informasiya təhlükəsizliyinin təminatı sahəsində dövlətlərin hüquqi tənzimetmə təcrübəsi və müasir informasiya sistemlərinin təhlükəsizliyinin hüquqi tənzimlənməsi istiqamətlərinin inkişafi məsələləri geniş şəkildə araşdırılır.

Dissertasiya işinin III fəsli "İnformasiya təhlükəsizliyinin hüquqi təminatı sferasında konstitusiya normaları və qanunvericiliyin sistemi" adlanır və iki yarımfəsildən ibarətdir. Burada Rusiya Federasiyası və Azərbaycan Respublikası praktikasında informasiya təhlükəsizliyinin təminatının hüquqi-qanunvericilik xüsusiyyətləri geniş və sistemli şəkildə, o cümlədən qarşılıqlı əsasda təhlil edilir.

"İnformasiya cəmiyyəti quruculuğunun hüquqi məsələləri" adlanan və üç yarımfəsildən ibarət dissertasiya işinin IV fəslində informasiya cəmiyyətinin inkişafının normativ əsasları, informasiya cəmiyyətinin informasiya təhlükəsizliyinin hüquqi tənzimlənməsinin təmin edilməsinin əsas istiqamətləri, informasiya təhlükəsizliyinin inkişafı dövründə elektron sənəd dövriyyəsinin həyata keçirilməsinin əsas istiqamətləri kimi mühüm məsələlər ətraflı şəkildə araşdırılır.

İki yarımfəsildən ibarət olan və "İnternet şəbəkəsində informasiya təhlükəsizliyinin təminatı" adlanan dissertasiya işinin V fəslində internet sisteminin fəaliyyətinin tarixi və müasir vəziyyəti, informasiyaya çıxışın hüquqi tənzimlənməsi və informasiya təhlükəsizliyinin təmin edilməsi xüsusiyyətləri nəzəri və praktik cəhətdən təhlil edilir.

Dissertasiya işinin nəticə hissəsində tədqiqatla əlaqədar əldə edilmiş mühüm təklif və nəticələr qeyd edilir, o cümlədən Azərbaycan Respublikası və Rusiya Federasiyası normativ hüquqi sistemi üçün onların nəzəri-praktik əhəmiyyəti ifadə edilir.

SUMMARY

Ramil Mahir oglu Aslanov's dissertation named "The theoretical and constitutional basis of the legal enforceability of information security in building the information society in the Republic of Azerbaijan and the Russian Federation" for attaining the degree of Doctor of Laws on the specialisation 5614.01 – "Administrative law; financial law; information law" is independent, creative and completed research, reflecting a completely new scientific provisions, devoted to extensive analysis of the legal issues of information security in the building of the information society, which is one of the interconnected actual problems of legal science of the Republic of Azerbaijan and the Russian Federation.

The dissertation is formed on the basis of a comparative analysis of the broad international universal, regional and bilateral treaty practice, the legislation of the various states, including the legislation of the Republic of Azerbaijan and the Russian Federation in the field of information security, as well as diverse points of views existing in legal literature and consists of an introduction, five chapters, conclusion and the list of used bibliography.

The introduction substantiates the relevance of the research, indicates the degree of elaboration, scientific novelty, new scientific provisions for the defense, goals and objectives, theoretical and practical significance of the research.

In the first chapter of the research, consisted of three paragraphs and called "Threats in the field of information and theoretical basis of the legal enforceability of information security", examines such important and topical issues as modern threats to information security and ways to overcome them, the concept of information security and its role in development of the information society, methodological problems of legal enforceability of information security.

The second chapter of the dissertation is called "Methods of legal enforceability of information security in the building of the information society" and is divided into three paragraphs. This chapter explores in detail the international legal regulation in the field of information security, the practice of States in the field of legal regulation of information security, including the development of directions of the legal enforceability of modern information systems.

The third chapter of the dissertation is called "Constitutional norms and the system of legislation on the legal enforceability of information security," and consists of two paragraphs. This chapter is widely and systematically, as well as on an interconnected basis analyzed the peculiarities of legal-legislative enforceability of information security in the Russian Federation and the practice of the Republic of Azerbaijan.

In the fourth chapter of the dissertation, entitled "Legal issues of building the information society" and consisted of three paragraphs, are analyzed in detail important issues such as the regulatory framework of the development of information society, the main directions of ensuring legal regulation of information security of the information society, the main directions of the electronic-documentary turnover in the stage of development of information security.

In the fifth chapter of the dissertation, consisted of two paragraphs and called "Information security in the Internet", on the theoretical and practical basis, the history and current state of operation of internet, legal regulation of access to information and particularly information security are analyzed.

The conclusion of the dissertation is comprised of suggestions that are made and results that are achieved in the end of the research, including the notes of their theoretical and practical importance for the normative system of the Russian Federation and the Republic of Azerbaijan.

AZƏRBAYCAN RESPUBLİKASI TƏHSİL NAZİRLİYİ
BAKI DÖVLƏT UNİVERSİTETİ

əlyazması hüququnda

RAMİL MAHİR OĞLU ASLANOV

AZƏRBAYCAN RESPUBLİKASI VƏ RUSİYA FEDERASİYASINDA İNFORMASİYA CƏMİYYƏTİ QURUCULUĞUNDA İNFORMASİYA TƏHLÜKƏSİZLİYİNİN HÜQUQİ TƏMİNATININ NƏZƏRİ VƏ KONSTİTUSİYA ƏSASLARI

İXTİSAS: 5614.01 – "İnzibati hüquq; maliyyə hüququ; informasiya hüququ"

Hüquq üzrə elmlər doktoru elmi dərəcəsi almaq üçün təqdim edilmiş dissertasiyanın

A V T O R E F E R A T I

BAKI – 2016