План

Введение

Глава 1. Защита информации в Российской Федерации

§1.1 Понятие и роль информации на современном этапе развития российского общества

§1.2 Защита информации - приоритетная задача обеспечения национальной безопасности России

Глава 2. Законодательная база, регулирующая отношения в сфере информационной безопасности

§2.1 Нормативно-правовые основы защиты информации в Российской Федерации

§2.2 Направления развития законодательства

§3. Информационное законодательство - основной источник информационного права

§4. Правовые проблемы информационной безопасности

Заключение

Список нормативных актов и литературы

## Введение

Актуальность. Конец ХХ и начало ХХI в. характеризуются новым этапом научно-технической революции - внедрением во все сферы жизни инфокоммуникационных технологий - необходимой базы для перехода к информационному обществу, оказывающих огромное влияние на все аспекты нашей жизни. Как отмечается в Декларации принципов построения информационного общества (Декларации тысячелетия) [[1]](#footnote-1), такие технологии открывают совершенно новые перспективы достижения более высоких уровней развития.

В настоящее время в Российской Федерации сформировались необходимые условия для перехода к информационному обществу. Это отмечается и в Стратегии развития информационного общества в России, одобренной на заседании Совета Безопасности Российской Федерации 25 июля 2007 г. (далее - Стратегия).

Стратегия является политическим документом и направлена на реализацию положений Окинавской Хартии глобального информационного общества[[2]](#footnote-2) и итоговых документов Всемирной встречи на высшем уровне по вопросам информационного общества (Женева, 2003 г., Тунис, 2005 г). В ней определены цели и принципы развития информационного общества в России, роль государства в данном процессе, предусмотрены основные мероприятия по достижению целей развития информационного общества в России.

Правовые проблемы регулирования информационных отношений при построении информационного общества в России в настоящее время нуждаются в тщательном исследовании, поскольку резко ускоряющиеся информационно-коммуникативные процессы глобализации эволюционируют в качественно новое состояние - режим реального времени. Возникающие в связи с этим новые общественные отношения нуждаются в адекватном правовом регулировании.

Одним из необходимых условий развития информационного общества является развитие системы нормативного правового регулирования отношений в области создания и использования информационно-телекоммуникационных технологий. В то же время будет справедливым признать, что именно общественные отношения в информационной сфере, пронизывающей сегодня практически все области жизнедеятельности человека, общества и государства, являются импульсом, влияющим на развитие информационного законодательства. Это послужило толчком к тому, чтобы выбрать тему курсовой работы, которая звучит как: правовые основы обеспечения информационной безопасности.

Объектом курсовой работы являются общественные отношения, возникающие вокруг правового регулирования сферы информационной безопасности.

Предметом же исследования будет являться нормативная правовая база, регламентирующая отношения, определенные объектом исследования.

Цель работы состоит в том, чтобы рассмотреть источники права, регулирующие отношения в сфере информационной безопасности, разобраться в полноте отражения ими существующих реалий общественной жизни, может быть, увидеть пробелы в законодательстве и предложить пути их решения.

Исходя из целей, ставлю перед собой задачи:

Разобраться с понятием информационная безопасность

Рассмотреть нормы права, регулирующие общественные отношения в сфере информационной безопасности

Отразить степень соответствия существующих норм реально имеющимся отношениям.

Сформулировать свои предложения по совершенствованию законодательства.

Структура курсовой работы. Курсовая работы традиционно состоит из следующих основных элементов: введение; две главы, содержащие ряд параграфов; заключение; список нормативных актов и литературы.

Положения, выносимые на защиту:

информационная безопасность проявляется через максимальную защищенность социально значимых институтов: экономики, бытовых условий, экологии, надлежащее обеспечение обороны государства.

информационная безопасность определяется способностью нейтрализовать воздействие по отношению к опасным, дестабилизирующим, деструктивным, ущемляющим интересы страны информационным воздействиям на уровне, как внедрения, так и извлечения информации.

## Глава 1. Защита информации в Российской Федерации

## §1.1 Понятие и роль информации на современном этапе развития российского общества

Основным объектом правоотношений в информационной сфере является информация. "Информация - это информация, а не энергия и не материя", - сказал Ноберт Винер - отец кибернетики. В его определении информация выступает как философская категория наравне с материей и энергией.

Понятно, что такое философское определение информации для права неприемлемо, как и неприемлемо, например, регулирование отношении по поводу энергии вообще или материи вообще. Информация как объект правоотношений должна быть конкретизирована, организована должным образом, "привязана" к ситуации и конкретному виду отношений, классифицирована по видам и тому подобным образом "подготовлена" для осуществления по ее поводу действий, регулируемых нормами права.

В практическом смысле, понятном каждому, определение информации дал С.И. Ожегов: [[3]](#footnote-3)

информация - это:

1) сведения об окружающем мире и протекающих в нем процессах;

2) сообщения, осведомляющие о положении дел, о состоянии чего-либо.

До середины 20-х гг. XX в. под информацией (в переводе с латыни - ознакомление, разъяснение, изложение) действительно понимались "сообщения и сведения", передаваемые людьми устным, письменным или другим способом. С середины XX в. информация определяется как общенаучное понятие, включающее обмен сведениями между людьми, человеком и автоматом, автоматом и автоматом; обмен сигналами в животном и растительном мире; передачу признаков от клетки к клетке, от организма к организму (генетическая информация), одно из основных понятий кибернетики. [[4]](#footnote-4)

В связи с развитием средств связи и телекоммуникаций, вычислительной техники и их использованием для обработки и передачи информации возникла необходимость измерять количественные характеристики информации. Появились разные теории, и понятие "информация" начало наполняться разным содержанием.

В 1949 г.К. Шеннон и У. Уивер опубликовали статью "Математическая теория связи", в которой были предложены вероятностные методы для определения количества передаваемой информации. Однако такие методы описывают лишь знаковую структуру информации и не затрагивают заложенного в ней смысла (в сообщении, сведениях).

В 1948 г.Н. Винер предложил "информационное видение" кибернетики как науки об управлении в живых организмах и технических системах. Под информацией стали понимать не просто сведения, а только сведения новые и полезные для принятия решения, обеспечивающего достижение цели управления. Остальные сведения не считались информацией.

Уже много лет развивается семантическая теория информации, которая изучает смысл, содержащийся в сведениях, полезность и ценность этих сведений для потребителя. В этой связи существенным становится субъективный подход, основанный и на априорной подготовленности субъекта к восприятию таких сведений или сообщений и с их новизной для субъекта и с их полезностью (или ценностью) для принятия им решений, направленных на достижение поставленных целей.

Термин "информация" и связанные с ним термины сегодня широко применяются и законодателем.

Федеральный закон "Об информации, информатизации и защите информации" определяет информацию как "сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления" (ст.2). Учитывая социальный аспект рассматриваемого предмета, добавим: в виде, понятном для восприятия человеком. Такое определение дает возможность "вывести" из понятия "информация" программы для электронных вычислительных машин (ЭВМ), отнесенные названным Законом к средствам обеспечения ЭВМ.

По роли в правовой системе информация разделяется на правовую и неправовую.

Нормативная правовая информация создается в порядке правотворческой деятельности и содержится в нормативных правовых актах. Классификация такой информации по уровню принятия актов или по видам актов приведена на рис.2.

Ненормативная правовая информация создается, как правило, в порядке правоприменительной и правоохранительной деятельности.

С помощью такой информации реализуются предписания правовых норм. Эта информация создается в объекте управления и движется в контуре обратной связи системы правового управления. К ненормативной правовой информации относятся:

1) общая информация о состоянии законности и правопорядка:

заявления, поступающие в прокуратуру. Конституционный Суд РФ, Верховный Суд РФ, Высший Арбитражный Суд РФ о соблюдении законности;

судебная, уголовная и прокурорская статистика;

информация о соблюдении прав и свобод человека (в том числе и по представлению Уполномоченного по правам человека);

социологические исследования об эффективности законодательных и иных нормативных правовых актов;

2) информация о гражданско-правовых отношениях, договорных и иных обязательствах (договоры, соглашения и т.п. документы);

3) информация, представляющая административную деятельность органов исполнительной власти и местного самоуправления по исполнению нормативных предписаний;

4) информация судов и судебных органов (судебные дела, судебные решения и т.п.);

5) информация, связанная с раскрытием и расследованием правонарушений:

криминологическая информация - данные о преступности и других правонарушениях, эффективности уголовных наказаний;

криминалистическая информация, используемая при доказательстве факта преступления и идентификации лица или группы лиц, совершивших преступление;

судебно-экспертная информация, используемая при проведении судебных экспертиз для доказательства факта преступления и вины обвиняемого;

оперативно-розыскная информация, содержащая сведения, отражающая ход и результаты оперативно-розыскных мероприятий по установлению и розыску лиц, совершивших уголовно-наказуемые деяния, а также иные сведения и материалы.

Из материала, изложенного выше, видно, что "информация" присуща абсолютно всем сферам жизни общества и никак не обойтись без защиты информации доступными правовыми, а вместе с ними и материальными средствами. Об этом пойдет речь в следующем параграфе.

## §1.2 Защита информации - приоритетная задача обеспечения национальной безопасности России

Ни одна сфера жизни современного общества не может функционировать без развитой информационной структуры. Проникая во все сферы деятельности государства, информация приобретает конкретные политическое, материальное и стоимостное выражения. На этом фоне все более актуальный характер приобретает в последние десятилетия и особенно в настоящее время задача обеспечения информационной безопасности Российской Федерации, как неотъемлемого элемента ее национальной безопасности, а защита информации превращается в одну из приоритетных государственных задач. Защита информации обеспечивается в любом государстве и в своем развитии проходит множество этапов в зависимости от потребностей государства, возможностей, методов и средств ее добывания (в частности разведки), правового режима государства и реальных его усилий по обеспечению защиты информации.

Важным этапом становления и совершенствования такой системы в нашей стране явился период 70-80-х гг. С начала 70-х гг. в разведывательной деятельности ведущих стран мира началось широкомасштабное применение технических средств разведки, 80-е гг., ознаменовавшись бурным научно-техническим прогрессом, особенно в военной области, дали новые импульсы в дальнейшем наращивании возможностей технических средств иностранных разведок: до 70% разведывательной информации добывалось в то время с помощью технических средств. Сложившаяся обстановка потребовала совершенствования системы мер противоборства с иностранными разведками. Противодействие техническим разведкам стало задачей государственной важности и одной из составных частей в общей системе мер по сохранению государственной и служебной тайны.

Для организации и координации работ в этой области решением правительства 18 декабря 1973 г. была создана Государственная техническая комиссия СССР. Тогда же начала формироваться система научного обеспечения комплексного противодействия иностранным техническим разведкам. В 1974 г были сформированы концептуальные, организационные, научно-методологические и нормативные основы противодействия иностранным техническим разведкам (ПДИТР) и развернута большая практическая работа. В 80-е гг. была разработана цельная концепция по противодействию иностранной технической разведке. Совершенствовались нормативная база, методы и средства контроля. К началу 90-х гг. произошли качественные изменения в военно-политической и научно-технической сферах, заставившие во многом пересмотреть государственную политику в области защиты информации в целом.

Во-первых, информационные технологии принципиально изменили объем и важность информации, обращающейся в технических средствах ее передачи и обработки.

Во-вторых, в России отошла в прошлое фактическая государственная монополия на информационные ресурсы, в частности получило конституционное закрепление право гражданина искать, получать и распространять информацию.

В-третьих, прежний административный механизм управления защитой информации стал и невозможен, и неэффективен, в то же время необходимость межведомственной координации в сфере защиты информации объективно возросла.

В-четвертых, завершилась острая военно-политическая конфронтация между СССР и странами НАТО, начавшееся контролируемое сокращение вооружений и развитие мер доверия в военной области потребовали обеспечить разумное сочетание мер открытости и мер по защите государственной тайны.

В-пятых, в связи с усиливающимся включением России в международное разделение труда, укреплением экономических, культурных, гуманитарных контактов с другими государствами многие режимно-ограничительные меры, облегчавшие защиту информации, например система регионов, закрытых для посещения иностранными гражданами, стали неприемлемы.

Следует особо отметить, что политическая ситуация, сложившаяся в мире в результате прекращения "холодной войны" между Западом и Востоком, по существу не затронула такого ее атрибута, как разведка. Ведущие западные страны продолжают модернизировать и развивать свои разведывательные службы, совершенствовать техническую разведку, наращивать ее возможности. Наряду с традиционными приоритетами иностранных технических разведок в сферу их интереса все в большей вовлекаются вопросы технологий, финансов, торговли, ресурсов, доступ к которым открывается в связи с конверсией, развитием международных интеграционных процессов, широким внедрением компьютерных технологий.

В этих условиях слепое следование оправдавшим себя в прошлом решениям непременно привело бы к ущербу государственным интересам России в военной, политической, экономической и других областях. Требовалось совершенствование как сложившейся системы защиты информации в организационном плане, так и концептуальных, методологических подходов к защите информации от иностранной технической разведки и от ее утечки техническим каналам.

Высшими органами государственной власти Российской Федерации был предпринят ряд принципиально важных шагов. В частности, Указом Президента в январе 1992 г. на базе Гостехкомиссии СССР был создан государственный орган более высокого статуса - Государственная техническая комиссия при Президенте Российской Федерации (Гостехкомиссия России) [[5]](#footnote-5).

В настоящее время большие изменения происходят в методологии защиты информации. Осуществляется переход от дорогостоящего скрытия заведомо завышенного объема данных к гарантированной защите принципиально важных, "узловых точек". Закладываются правовые основы такой деятельности. Приняты Закон Российской Федерации "О государственной тайне"[[6]](#footnote-6) и Федеральный закон "Об информации, информатизации и защите информации"[[7]](#footnote-7). Этими правовыми актами сферу защиты информации распространен такой основополагающий принцип, как баланс интересов государства, общества и личности.

Произошло структурное совершенствование существующей системы органов защиты государственной тайны. Ее основным элементом стала Межведомственная комиссия по защите государственной тайны, предназначенная для координации всей деятельности органов государственной власти, предприятий, учреждений организаций в этой области. Одними из главных результатов этой деятельности явились подготовка и утверждение Президентом Российской Федерации Перечня сведений, отнесенных к государственной тайне, и государственной программы по обеспечению защиты государственной тайны на 1996-1997 гг. Опубликование в открытой печати "Перечня сведений, отнесенных к государственной тайне", открыло новый этап в обеспечении защиты информации, составляющей государственную тайну, явилось реальным результатом демократизации России в части открытости и гласности.

## Глава 2. Законодательная база, регулирующая отношения в сфере информационной безопасности

## §2.1 Нормативно-правовые основы защиты информации в Российской Федерации

Государственная политика в Российской Федерации по обеспечению информационной безопасности реализуется через правотворчество, правоприменение и участие государства в развитии правосознания и правовой культуры граждан.

При издании Свода законов СССР в 1970-х гг. насчитывалось 29 тысяч действующих законов, подлежащих систематизации, и более одного миллиона подзаконных нормативно-правовых актов, при этом 120 союзных министерств и ведомств ежегодно издавали до 300 таких актов. За последние 10 лет в России принято более 1000 законов, что намного превосходит прежние темпы законотворчества.

За последние годы российское законодательство существенно обновилось. Особенно это коснулось тех сфер правового регулирования, где приняты кодифицированные акты, в том числе Гражданский, Налоговый, Бюджетный, Семейный, Уголовный, Водный и Лесной, Земельный, Трудовой, Гражданский процессуальный и Уголовно-процессуальный кодексы, Кодекс об административных правонарушениях. С их принятием появились реальные условия для проведения полноценной систематизации законодательства и издания Свода законов России.

При формировании законодательства в информационной сфере в самостоятельную отрасль, формирующееся законодательство в сфере обеспечения информационной безопасности является подотраслью информационного законодательства, а при его кодификации в случае принятия Информационного кодекса Российской Федерации может стать его составной частью. Сегодня же, признавая информационное право в качестве отрасли российского права, следует учитывать, что ему не соответствует в законодательстве информационное законодательство в качестве отрасли российского законодательства и его формирование является делом трудным, рассчитанным, по-видимому, на долгие годы. В настоящее время уже существует концепция развития законодательства в сфере информационной безопасности. Положения концепции одобрены на парламентских слушаниях в Государственной Думе РФ, на заседании Комитета Государственной Думы РФ по безопасности в ноябре 1998 г. и предполагают принятие более 20 новых законов и внесение изменений и дополнений в 50 действующих законов, работа над которыми ведется в настоящее время. Межведомственная комиссия Совета Безопасности РФ по информационной безопасности своим решением от 2 декабря 1997 г. отметив, что существующее правовое регулирование отношений в области обеспечения информационной безопасности не соответствует современным требованиям и препятствует формированию эффективной системы информационной безопасности Российской Федерации, определила следующие основные направления развития законодательства в области обеспечения информационной безопасности:

внесение изменений и дополнений в действующее законодательство для развития обеспечения информационной безопасности в целях устранения противоречий нормам Конституции РФ и международным соглашениям, к которым присоединилась РФ, противоречий между законодательными актами федерального уровня и актами субъектов РФ, а также конкретизации норм ответственности за правонарушения в области информационной безопасности;

законодательное разграничение уровней правового регулирования проблем обеспечения информационной безопасности (федеральный уровень, уровень субъекта Федерации, уровень местного самоуправления);

создание нормативно-правовой базы для развития системы страхования информационных рисков, направленной на гарантированное обеспечение страховой защиты как пользователей информационных услуг, так и субъектов, предоставляющих такие услуги; уточнение правового статуса иностранного инвестора при инвестировании в отрасль связи и информатизации в интересах обеспечения национальной безопасности Российской Федерации;

законодательное закрепление приоритета развития национальных сетей связи и отечественного производства космических спутников связи;

разработка Национальной программы развития общедоступных компьютерных сетей, включая определение правового статуса провайдеров интернет-услуг и правовое регулирование их деятельности, представление в Интернет информации о деятельности органов государственной власти и органов местного самоуправления, защиту русского языка в Интернете;

создание правовой базы для функционирования в Российской Федерации системы региональных центров обеспечения информационной безопасности;

правовое регулирование развития негосударственного компонента в формировании информационного общества и обеспечении информационной безопасности Российской Федерации.

## §2.2 Направления развития законодательства

Не перечисляя принятые законы и другие нормативно-правовые акты в области регулирования отношений в информационной сфере, можно отметить некоторые позитивные сдвиги и проблемы по трем направлениям. К таким важным для оценки состояния отрасли относятся вопросы:

каково воздействие нормативно-правовой основы на оформление производственно-научной инфраструктуры информатики и функционирование ее как отрасли российской экономики, как особого вида социально-экономической деятельности;

что дает потребителю современная российская информатика в совокупности информационных ресурсов, информационных технологий и коммуникаций и как обеспечиваются права граждан в области информатизации;

какие стороны информационной сферы являются наиболее чувствительными с точки зрения правового обеспечения информационной безопасности.

За последние годы в этой области можно наблюдать значительные сдвиги под влиянием реальных процессов информатизации. Правовой основой здесь является Федеральный закон "Об информации, информатизации и защите информации"[[8]](#footnote-8), которым наиболее детально урегулированы вопросы правового режима информационных ресурсов.

На основе положений названного Закона создана нормативно-правовая база информатизации субъектов Российской Федерации. Информационные ресурсы обрели значительную основу для их организации и развития в региональных, территориальных, отраслевых и межотраслевых системах.

Правовая наука пока не может остановиться на какой-либо определенной модели в области регулирования и защиты интеллектуальной собственности и особенно исключительных прав создателей информационного и технологического продукта. Тем не менее, закон должен откликаться на коллизии в этой среде. Речь идет о том, что в процессе дополнений и изменений базового Закона и законов субъектов России необходимо уделить большее внимание означенным вопросам. Важное направление работы и области создания адекватной инфраструктуры в сфере информатики формируется вокруг создания и использования таких объектов, как информационные технологии и вычислительная техника.

Преодоление немалого отрыва от передовых стран, несмотря на имеющиеся значительные заделы по технической базе макросистем, требует организации и стимулирования производства в области технологий. В данном блоке проблем особого внимания требуют вопросы:

программирования и создания продукции по мировым стандартам особенно для открытых систем деловой информации;

формирование рынка этой продукции;

регулирование отношений в области информационной деятельности, информационных услуг, организации и обеспечения ответственности различных посреднических структур в информационных и коммуникационных системах.

Правовые решения в этой части проблем касаются тематики собственности ни информационную продукцию, программное обеспечение, пресечения выноса на рынок контрафактной продукции. Вопросы авторского права на информационные технологии и программное обеспечение требуют внимания не меньшего, чем в области информационных технологий.

Важнейшее направление законотворчества представляют проблемы обеспечения интересов пользователей, потребителей продукции современных технологий и ресурсов.

В этой части формирования контуров информационного общества на первом плане находятся проблемы включения и использования информационных технологий в сферы социальной, политической, культурной, производственной, научной, управленческой деятельности. Сюда же относятся и вопросы создания условий массового информирования населения.

Известно, что все развитые страны формируют правительственные программы использования информационных технологий в основных сферах общественной жизни. Это касается в первую очередь обслуживания электронной торговли, электронизации управления, широкого использовании информационных технологий в сфере образования, культуры, средств массовой информации. Но наиболее остро стоит вопрос об отставании в использовании информационных технологий в структурах государственного управления. И дело отнюдь не в количестве компьютеров, которые приходятся на одного служащего. Дело в том, что большинство компьютеров в открытых системах до сих пор не увязано в единые сети и не обеспечивают активного перехода на электронные документы и современный документооборот. Право и политика органов исполнительной власти пока не предоставляет необходимых инноваций в этой области.

Необходимо подчеркнуть, что информатизация в области государственного управления должна стать органической частью административной реформы и реформы экономической.

При этом в основе должно быть заложено требование о гуманизации целей информатики. Социальные интересы, гармония интересов общества, личности, государства должны быть сбалансированы и нацелены на обеспечение тех потребностей общества, которые позволяют отдать приоритет повышению уровня культуры, сохранению цивилизации в подлинном ее понимании.

Следует также уделить внимание вопросу, какие участки в области государственного аппарата и всей управленческой деятельности можно считать наиболее чувствительными для информационной безопасности.

Концепция нормативно-правового обеспечения информационной безопасности базируется на Доктрине информационной безопасности (8), которая ориентирует на выделение четырех основных составляющих национальных интересов России в информационной сфере:

соблюдение прав и свобод и гражданина в области получения информации и пользования ею при соблюдении гарантий в области персональных данных и личных тайн;

информационное обеспечение государственной политики Российской Федерации, формирование достоверной информации о политике государства при обеспечении баланса интересов общества, государства, личности;

развитие современных информационных технологий, отечественной индустрии информации, индустрии средств информатизации, коммуникаций и связи, формирование рынка на эти виды продукции;

защиту информационных ресурсов от несанкционированного доступа, обеспечение безопасности информационных и телекоммуникационных систем на территории России.

Каждое из этих направлений наполняется конкретными задачами, которые предстоит решать с помощью не только правовых средств и методов, но и колоссальной организационной работы и технологической базы.

Защитная реакция и превентивные меры свойственны и органам надзора в области информатизации. Стремление выхода в Интернет различных органов и организаций, что стимулируется самой жизнью, требует регулирования поведения ответственных лиц и правил, которые непременно должны соблюдать все субъекты. Новое явление порождает и новые проблемы для общества. Однако можно наблюдать тактику надзорных органов, которая сводится к применению механизмов воздействия, не адаптированных к новым условиям. Просто "закрыть" или "наказать" - мало. В данном случае имеем в виду ситуацию, которая складывается в связи с новыми формами работы публичных библиотек, специальных информационных систем. Закрыть сайт еще не означает обеспечить порядок отношений. Следует активно ставить вопрос и действовать в направлении выработки новых норм и правовых актов, соответствующих современным условиям.

Важное значение в области информатики приобретают два не совсем правовых направления. Но они тесно связаны с правом и нуждаются в его поддержке. Во-первых, область бурно развивающихся стандартов технических и организационных. Они формируются преимущественно в региональном и международном фарватере, но их включение в регулятивные механизмы требует внимания и со стороны законодательства.

Во вторых, набирают силу и акты, имеющие морально-нравственную основу. Здесь необходима тщательная работа по взаимодействию правовых и нравственно-этических норм. Это задача аналитики в области исследования социальных нормативных регуляторов, в структуре которых возможно наращивание потенциала контроля непосредственно со стороны общества. Различные кодексы чести, долга и т.п. акты следует поощрять, но при этом и контролировать, имея в виду уязвимость сферы общественного сознания, которая под любыми предлогами может использоваться заинтересованными деструктивными силами.

Достаточно чувствительной стороной состояния законодательства в области практической информатики являются проблемы процессуального значения. Это огромная область науки и практики, так как необходимы новые решения в учете, фиксации, сборе доказательств, в выработке оценки юридических фактов и их слагаемых, в понимании тонкостей работы с информацией в разных областях жизни. Процедуры и правила работы с информацией в системах государственного управления и в деловой практике частного сектора, процессуальные правила правоохранительных органов - особая область законодательства.

Важен еще один момент. Уделив внимание вопросам юридической техники в плане теории права, необходимо подчеркнуть, что это исключительная по значимости область и законотворчества. Информатика здесь дает новые инструментарии, и научиться их использовать - одна из задач юридических служб во всех структурах, принимающих решения и особенно в области создания новых нормативных актов.

Специфика сферы правового регулирования и обеспечения информационной безопасности заключается в том, что здесь необходима уравновешенность между профилактической и непосредственной работой по обеспечению безопасных условий развития сферы информатизации и информатики в целом. Профилактика осуществляется на основе правового обеспечения нормальных условий работы. Пробелы или противоречия на этой стадии порождают угрозы, проистекающие из самой системы информатизации и из среды потребителей продукции и услуг информатики. Все те недоработки в области правового регулирования и неупорядоченности организации сфер и производства информации, сфер социальной жизни обслуживания информационно-коммуникативным ресурсом, о которых уже сказано, являются источником угроз в области информационной безопасности.

Собственно сфера информационной безопасности в значительной мере связана с обеспечением учета, анализа причин возникновения конфликтов и угроз налаженному порядку отношений как в открытой, так и в ограниченной но доступу сфере информатики. Здесь видна непосредственная связь со всем спектром национальной безопасности и информационным его обеспечением. Специалисты отмечают следующий набор причин обострения безопасности: вызов, риск, угроза, опасность, страх. Вызовы могут исходить из внутренней среды государства (реформы, преобразования в темпах, которые общество не успевает переварить), а также из среды внешней - монополизация, приоритеты в сфере производства, потребления, влекущие нарушение внутренних балансов или излишнее напряжение в той или иной сфере развития. Кроме того, риски в значительной мере сопряжены с неупорядоченностью отношений. Так можно рассматривать каждую позицию с профессиональной точки зрения и на этом строить систему обеспечения безопасности. Отметим только, что позиция обороны, снятия последствий мало продуктивна. Преимущество обеспечения безопасности все же коренится в области профилактики и создания нормального течения процессов. Эти рассуждения важны для расстановки акцентов в правовой работе, и в первую очередь в нормотворческой деятельности соответствующих органов государственной власти.

Решение проблем информационной безопасности предполагает и наличие общего правового регулирования отношений в рассматриваемой сфере, на основе которого создаются условия нормального режима работы и отношений, исключающие или сокращающие угрозы, опасность правонарушений.

Если исходить из понимания безопасности как создание определенного состояния системы, то задача обеспечения безопасности достигается в процессе создания нормального состояния информационных ресурсов, состоянии реализации права на информацию различных субъектов, развития инфраструктуры информатизации и т.д. Следовательно, в каждом предметном направлении правового регулирования и формирования нормативно-правовой основы совмещаются задачи создания условий бесконфликтных отношений участников и одновременно условий предотвращения отступлении от нормы, выявления угроз и опасностей по каждому направлению, а также по формированию механизмов реагирования на реализуемые отступления от установленных правил. В целях анализа полноты, эффективности норм, обеспечивающих выявление угроз, правонарушений (что свидетельствует об опасности), применения мер ответственности в этих случаях в структуре направлений правового регулирования, возможно выделить "обеспечение информационной безопасности". Но в самом законодательстве обозначить границу между актами и нормами, посвященными отдельно общему регулированию отношений и обеспечению безопасности в информационной сфере почти невозможно. Каждый закон, каждый иной нормативный акт содержит нормы, обеспечивающие правила, порядок отношений, соблюдение которых создает состояние безопасности, а нарушение или отступление от них - условия угрозы или реального правонарушения. Если в организационных и технических мерах возможно выделить специально предназначенные для реализации обеспечения безопасности, защиты от угроз внутренних и внешних, то в правовых отношениях материя не поддается такому механическому разделению.

Представляется, что каждый правовой акт может быть оценен не только с позиций позитивного установления правил поведения или отношений, но и с позиций его потенциала предотвращения нарушений. Для достижения целей безопасности чаще применяются запретительные нормы, условия ограничения дозволенного. Известно, что состав правонарушений и санкции помещаются в соответствующие кодексы, нормы которых не всегда гармонизированы с нормами регулятивного характера.

Много проблем связано и с механизмами выявления, фиксации правонарушений, их расследования, с осуществлением экспертиз и судебного разрешения дел. Здесь формируется область ответственности, которую можно рассматривать как наиболее самостоятельную область правового обеспечения безопасности: пресечение нарушения, восстановление нарушенного права, выбор меры наказания и т.д. В связи с этим в области правового обеспечения информационной безопасности первостепенное значение приобретают нормы процессуального права.

Можно отметить, что эффективность законодательства определяется полноценностью его регулятивной части - той части норм, которые создают ясность у участников определенных отношений, как они должны действовать в той или иной ситуации, какими правами и обязанностями они наделены от имени государства или своего контрагента (партнера). В этих целях всякий раз необходимо знать о наличии нормативной основы для тех или иных отношений. Обращение практики к массиву действующего законодательства и подзаконных актов в информационной сфере часто завершается установлением неполноты, несогласованности, а порой и противоречивости нормативно-правовой основы.

## §3. Информационное законодательство - основной источник информационного права

Вопросы, связанные с информационным законодательством требуют отражения внимания государства к ряду направлений деятельности в области информатизации. Можно отметить из них наиболее очевидные.

Формирование информационных ресурсов и развитие информационной деятельности - деятельности, непосредственно связанной со сбором, хранением, обработкой, передачей информации в самых разных организационных формах (документированная, звуковая, световая, цифровая и т.п.); деятельности по созданию средств обработки информации в электронном виде - создание программ, программного обеспечения и иных средств работы с информацией и ее транспортировкой (коммуникацией) по каналам связи, сетям в соответствии с типами организации информационных систем и сетей на основе современных технических и технологических достижений; управление качеством информационных технологий (достоверность, полнота, неуязвимость передаваемой информации и создание средств ее защиты в системах информационной безопасности); организация рынка информационных технологий. Все эти направления могут быть объединены в блок формирования специальной отрасли информатики, объединяющей проблемы создания, производства и использования средств информатизации, информационных технологий в широком понимании.

Вторым крупным блоком в системе государственного управления является деятельность по организации применения средств информатизации и информационных ресурсов в самых разных сферах социального развития.

Здесь сосредоточены проблемы информатизации экономики, экологии, здравоохранения, любых отраслей производства, науки, образования, культурно-просветительской деятельности, формирования и использования соответствующих видов и форм информационных ресурсов. Сюда же входят проблемы региональной и отраслевой информатизации и формирование специальных отраслей государственного управления в данной сфере.

Пока на уровне системы федеральных органов исполнительной власти функционирует федеральный органа, непосредственно выполняющий функции государственного управления - это Министерство связи и информатизации РФ. Кроме того, действуют специализированные государственные органы, ориентированные на организацию и использование отдельных массивов информационного ресурса. Это Архивная служба РФ, органы федеральной статистики. Государственная техническая комиссия. Большое внимание информационным проблемам уделяет Совет Безопасности РФ.

Это направление охватывает процессы информатизации деятельности органов государственной власти и местного самоуправления и их взаимодействия. Деятельность органов государственной власти - законодательных, исполнительных, правоохранительных - только и может быть продуктивной и эффективной при условии применения информационных технологий в работе аппарата каждого органа и в системе взаимодействия различных органов между собой.

Четвертый блок в сфере государственного управления в области информационных технологий составляет деятельность каждого из ведомств и государственных организаций, которые самостоятельно и с учетом своих потребностей обеспечивают процессы информационного обеспечения своей деятельности. При отсутствии должной координации на уровне федерации это направление деятельности подвержено местничеству и заканчивается неоправданной тратой средств, несовместимостью средств информатизации, в том числе и информационных технологий в едином пространстве страны.

Поддержка процессов информатизации во всех секторах хозяйства и культуры страны, во всех сферах социального развития и жизнеобеспечения; привлечение населения к новым методам работы с информацией на основе воспитания информационной культуры, переподготовки кадров и массового обучения молодого поколения работе в новых условиях. Здесь сосредоточены организационно-правовые проблемы обеспечения реализации права на информацию различных субъектов, разрешение конфликтов в области формирования и использования информационных технологий.

Все обозначенные направления государственного управления в области информационных технологий реализуются на основе создания и применения соответствующих законов и иных правовых актов, введения обязательных государственных стандартов, методик и правил.

## §4. Правовые проблемы информационной безопасности

Законом РФ "О безопасности"[[9]](#footnote-9) безопасность определяется как состояние защищенности жизненно важных интересов личности, общества и государства.

Жизненно важные интересы определяются законодателем как совокупность потребностей, удовлетворение которых обеспечивает существование и возможности прогрессивного развития личности, общества, государства, а угроза безопасности - как совокупность условии и факторов, создающих опасность жизненно важным интересам личности, общества, государства. И, наконец, обеспечение безопасности - проведение единой государственной политики в этой сфере и система мер экономического, политического, организационного и иного характера, адекватных угрозам жизненно важным интересам личности, общества и государства, направленных на выявление и предупреждение угроз.

Как уже упоминалось, Федеральным законом "Об участии в международном информационном обмене" определено понятие информационной безопасности как состояние защищенности информационной среды общества, обеспечивающее ее формирование, использование и развитие в интересах граждан, организаций, государства.

В соответствии с предписаниями Федерального закона "Об информации, информатизации и защите информации" целями защиты информационной сферы являются (ст. 20):

предотвращение утечки, хищения, утраты, искажения, подделки информации;

предотвращение угроз безопасности личности, общества, государства;

предотвращение несанкционированных действий по уничтожению, модификации, искажению, копированию, блокированию информации; предотвращение других форм незаконного вмешательства в информационные ресурсы и информационные системы, обеспечение правового режима документированной информации как объекта собственности;

защита конституционных прав граждан на сохранение личной тайны и конфиденциальности персональных данных, имеющихся в информационных системах;

сохранение государственной тайны, конфиденциальности документированной информации в соответствии с законодательством;

обеспечение прав субъектов в информационных процессах и при разработке, производстве и применении информационных систем, технологий и средств их обеспечения.

В результате сопоставительного анализа области информационной безопасности информационной сферы (см. гл.2) с учетом положений Доктрины информационной безопасности и норм информационного законодательства в этой области можно выделить три основных направления правовой защиты объектов в информационной сфере (правового обеспечения информационной безопасности).

1. Первое направление. Защита чести, достоинства и деловой репутации граждан и организаций; духовности и интеллектуального уровня развития личности; нравственных и эстетических идеалов; стабильности и устойчивости развития общества; информационного суверенитета и целостности государства от угроз воздействия вредной, опасной, недоброкачественной информации, недостоверной, ложной информации, дезинформации, от сокрытия информации об опасности для жизни личности, развития общества и государства, от нарушения порядка распространения информации.

2. Второе направление. Защита информации и информационных ресурсов прежде всего ограниченного доступа (все виды тайн, в том числе и личной тайны), а также информационных систем, информационных технологий, средств связи и телекоммуникаций от угроз несанкционированного и неправомерного воздействия посторонних лиц.

3. Третье направление. Защита информационных прав и свобод личности (право на производство, распространение, поиск, получение, передачу и использование информации; права на интеллектуальную собственность; права собственности на информационные ресурсы и на документированную информацию, на информационные системы и технологии) в информационной сфере в условиях информатизации. Рассмотрим их подробнее.

10.2. Правовая защита интересов личности, общества, государства от угроз воздействия недоброкачественной информации, от нарушения порядка распространения информации

Правовую основу первого направления правового обеспечения информационной безопасности составляют следующие информационно-правовые нормы Конституции РФ.

"Статья 29

5. Гарантируется свобода массовой информации. Цензура запрещается".

Законодатель имеет в виду, что свобода массовой информации и запрет цензуры дают возможность создавать и распространять достоверную, своевременную, объективную, т.е. доброкачественную информацию, при которой должно быть исключено распространение вредной и опасной информации (см. содержание первого направления). Именно такие требования с точки зрения информационной безопасности должны применяться при формировании института массовой информации, учитываться при подготовке нормативных правовых актов в рамках этого института.

"Статья 41

3. Сокрытие должностными лицами фактов и обстоятельств, создающих угрозу для жизни и здоровья людей, влечет за собой ответственность в соответствии с федеральным законом".

Эта норма прямого действия защищает личность и общество от сокрытия опасной информации.

"Статья 29

2. Не допускаются пропаганда или агитация, возбуждающие социальную, расовую, национальную или религиозную ненависть и вражду. Запрещается пропаганда социального, расового, национального, религиозного или языкового превосходства".

Это тоже норма прямого действия: защищает личность и общество от вредной и опасной информации конкретного, указанного вида.

Ответственность за распространение недоброкачественной информации, за нарушения порядка распространения информации предусматривается нормами УК РФ. Это клевета (ст.129), оскорбление (ст.130), воспрепятствование законной профессиональной деятельности журналистов (ст.144), заведомо ложная реклама (ст.182), злоупотребления при выпуске ценных бумаг (эмиссии) (ст.185), заведомо ложное сообщение об акте терроризма (ст. 207), сокрытие информации об обстоятельствах, создающих опасность для жизни или здоровья людей (ст.237), незаконное распространение порнографических материалов или предметов (ст.242), публичные призывы к насильственному изменению конституционного строя РФ (ст.280), возбуждение национальной, расовой или религиозной вражды (ст.282), публичные призывы к развязыванию агрессивной войны (ст.354).

Нормы об ответственности за административные правонарушения содержатся в Кодексе Российской Федерации об административных правонарушениях. Это, например, нарушение установленного порядка опубликования документов, связанных с подготовкой и проведением выборов, референдумов, нарушение правил проведения предвыборной агитации, агитации при проведении референдума в периодических печатных изданиях и на каналах организаций, осуществляющих теле - и (или) радиовещание, изготовление или распространение анонимных агитационных материалов, непредоставление или неопубликование отчета, сведений о поступлении и расходовании средств на подготовку и проведение выборов, референдума, непредоставление сведений об итогах голосования, нарушение порядка изготовления и распространения продукции средства массовой информации.

Завершая рассмотрение первого направления правового обеспечения информационной безопасности, обратим внимание на то, что защита от воздействия недоброкачественной информации сосредоточена главным образом в нормах законодательства о средствах массовой информации, нормах Уголовного кодекса РФ и КоАП.

10.3. Правовая защита информации, информационных ресурсов и информационных систем от угроз несанкционированного и неправомерного воздействия посторонних лиц

Правовую основу второго направления информационной безопасности составляют следующие информационные конституционные нормы.

"Статья 29

4. Перечень сведений, составляющих государственную тайну, определяется федеральным законом".

Конституция РФ охраняет личную тайну, информацию о личности или персональные данные от вмешательства посторонних лиц.

"Статья 23

1. Каждый имеет право на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени.

2. Каждый имеет право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений..."

При этом прямо запрещается кому бы то ни было собирать информацию о любом гражданине без его на то согласия.

"Статья 24

1. Сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются".

Конституцией РФ запрещается также получать иную информацию от любого гражданина без его добровольного на то согласия или убеждать его отказаться от предоставленной ранее информации.

Основной системообразующий набор норм, обеспечивающих защиту информации, информационных ресурсов, информационных систем от неправомерного вмешательства третьих лиц, развивающих содержание конституционных норм, содержится в Федеральном законе "Об информации, информатизации и защите информации".

"Статья 21. Защита информации

1. Защите подлежит любая документированная информация, неправомерное обращение с которой может нанести ущерб ее собственнику, владельцу, пользователю и иному лицу.

Режим защиты информации устанавливается:

в отношении сведений, отнесенных к государственной тайне, - уполномоченными органами на основании Закона Российской Федерации "О государственной тайне";

в отношении конфиденциальной документированной информации - собственником информационных ресурсов или уполномоченным лицом на основании настоящего Федерального закона;

в отношении персональных данных - федеральным законом".

К конфиденциальной информации относятся:

сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (персональные данные), за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях;

сведения, составляющие тайну следствия и судопроизводства;

служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом РФ и федеральными законами (служебная тайна);

сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией РФ и федеральными законами (врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений и т.д.);

сведения, связанные с коммерческой деятельностью, доступ к которым ограничен в соответствии с Гражданским кодексом РФ и федеральными законами (коммерческая тайна);

сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации информации о них.

2. Органы государственной власти и организации, ответственные за формирование и использование информационных ресурсов, подлежащих защите, а также органы и организации, разрабатывающие и применяющие информационные системы и информационные технологии для формирования и использования информационных ресурсов с ограниченным доступом, руководствуются в своей деятельности законодательством РФ.

3. Контроль за соблюдением требований к защите информации и эксплуатацией специальных программно-технических средств защиты, а также обеспечение организационных мер защиты информационных систем, обрабатывающих информацию с ограниченным доступом в негосударственных структурах, осуществляются органами государственной власти. Контроль осуществляется в порядке, определяемом Правительством РФ.

4. Организации, обрабатывающие информацию с ограниченным доступом, которая является собственностью государства, создают специальные службы, обеспечивающие защиту информации.

5. Собственник информационных ресурсов или уполномоченные им лица имеют право осуществлять контроль за выполнением требований по защите информации и запрещать или приостанавливать обработку информации в случае невыполнения этих требований.

6. Собственник или владелец документированной информации вправе обращаться в органы государственной власти для оценки правильности выполнения норм и требований по защите его информации в информационных системах. Соответствующие органы определяет Правительство РФ. Эти органы соблюдают условия конфиденциальности самой информации и результатов проверки".

Федеральным законом "Об информации, информатизации и защите информации" устанавливаются права и обязанности субъектов в области защиты информации.

"Статья 22. Права и обязанности субъектов в области защиты информации

1. Собственник документов, массива документов, информационных систем или уполномоченные им лица... устанавливают порядок предоставления пользователю информации с указанием места, времени, ответственных должностных лиц, а также необходимых процедур и обеспечивают условия доступа пользователей к информации.

2. Владелец документов, массива документов, информационных систем обеспечивает уровень защиты информации в соответствии с законодательством Российской Федерации.

3. Риск, связанный с использованием несертифицированных информационных систем и средств их обеспечения, лежит на собственнике (владельце) этих систем и средств.

Риск, связанный с использованием информации, полученной из несертифицированной системы, лежит на потребителе информации.

4. Собственник документов, массива документов, информационных систем может обращаться в организации, осуществляющие сертификацию средств защиты информационных систем и информационных ресурсов, для проведения анализа достаточности мер защиты его ресурсов и систем и получения консультаций.

5. Владелец документов, массива документов, информационных систем обязан оповещать собственника информационных ресурсов и (или) информационных систем о всех фактах нарушения режима защиты информации".

Законом предусматривается защита прав субъектов в сфере информационных процессов и информатизации.

"Статья 23. Защита прав субъектов в сфере информационных процессов и информатизации

1. Защита прав субъектов в сфере формирования информационных ресурсов, пользования информационными ресурсами, разработки, производства и применения информационных систем, технологий и средств их обеспечения осуществляется в целях предупреждения правонарушений, пресечения неправомерных действий, восстановления нарушенных прав и возмещения причиненного ущерба.

2. Защита прав субъектов в указанной сфере осуществляется судом, арбитражным судом, третейским судом с учетом специфики правонарушений и нанесенного ущерба.

3. За правонарушения при работе с документированной информацией органы государственной власти, организации и их должностные лица несут ответственность в соответствии с законодательством РФ и субъектов Российской Федерации.

Для рассмотрения конфликтных ситуаций и защиты прав участников в сфере формирования и использования информационных ресурсов, создания и использования информационных систем, технологий и средств их обеспечения могут создаваться временные и постоянные третейские суды.

Третейский суд рассматривает конфликты и споры сторон в порядке, установленном законодательством о третейских судах.

4. Ответственность за нарушения международных норм и правил в области формирования и использования информационных ресурсов, создания и использования информационных систем, технологий и средств их обеспечения возлагается на органы государственной власти, организации и граждан в соответствии с договорами, заключенными ими с зарубежными фирмами и другими партнерами с учетом международных договоров, ратифицированных Российской Федерацией".

Ответственность за правонарушения по этому направлению информационной безопасности регулируются нормами статей УК РФ: нарушение неприкосновенности частной жизни (ст.137), нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений (ст.138), незаконный экспорт технологий, научно-технической информации и услуг, сырья, материалов и оборудования, используемых при создании оружия массового поражения, вооружения и военной техники (ст.189), неправомерный доступ к компьютерной информации (ст.272), создание, использование и распространение вредоносных программ для ЭВМ (ст.273), нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети (ст.274).

Примером нормы об ответственности в Кодексе РСФСР об административных правонарушениях является ст.4014 "Умышленное уничтожение, повреждение печатных материалов, относящихся к выборам, референдуму".

В целом вопросы этого направления правового обеспечения информационной безопасности условно разделяются на защиту открытой информации и защиту информации ограниченного доступа.

Защита открытой информации осуществляется нормами института документированной информации

Защита информации ограниченного доступа регулируются нормами: института государственной тайны, института коммерческой тайны, института персональных данных, а также нормами защиты других видов тайн.

По третьему направлению Конституция РФ защищает от угроз информационной безопасности следующие информационные права и свободы.

"Статья 29

4. Каждый имеет право свободно искать, получать, передавать, производить и распространять информацию любым законным способом"

"Статья 33

Граждане Российской Федерации имеют право обращаться лично, а также направлять индивидуальные и коллективные обращения в государственные органы и органы местного самоуправления".

"Статья 29

1. Каждому гарантируется свобода мысли и слова".

"Статья 44

1. Каждому гарантируется свобода литературного, художественного, научного, технического и других видов творчества, преподавания. Интеллектуальная собственность охраняется законом.

2. Каждый имеет право на участие в культурной жизни и пользование учреждениями культуры, на доступ к культурным ценностям".

"Статья 29

"3. Никто не может быть принужден к выражению своих мнений и убеждений или отказу от них".

Отдельные положения конституционных норм развиваются нормами Федерального закона "Об информации, информатизации и защите информации".

"Статья 12. Реализация права на доступ к информации из информационных ресурсов

1. Пользователи - граждане, органы государственной власти, органы местного самоуправления, организации и общественные объединения - обладают равными правами на доступ к государственным информационным ресурсам и не обязаны обосновывать перед владельцем этих ресурсов необходимость получения запрашиваемой ими информации. Исключение составляет информация с ограниченным доступом...

2. Владельцы информационных ресурсов обеспечивают пользователей (потребителей) информацией из информационных ресурсов на основе законодательства, уставов указанных органов и организаций, положений о них, а также договоров на услуги по информационному обеспечению..."

"Статья 24. Защита права на доступ к информации

1. Отказ в доступе к открытой информации или предоставление пользователям заведомо недостоверной информации могут быть обжалованы в судебном порядке.

Неисполнение или ненадлежащее исполнение обязательств по договору поставки, купли-продажи, по другим формам обмена информационными ресурсами между организациями рассматриваются арбитражным судом.

Во всех случаях лица, которым отказано в доступе к информации, и лица, получившие недостоверную информацию, имеют право на возмещение понесенного ими ущерба.

2. Суд рассматривает споры о необоснованном отнесении информации к категории информации с ограниченным доступом, иски о возмещении ущерба в случаях необоснованного отказа в предоставлении информации пользователям или в результате других нарушений прав пользователей.

3. Руководители, другие служащие органов государственной власти, организаций, виновные в незаконном ограничении доступа к информации и нарушении режима защиты информации, несут ответственность в соответствии с уголовным, гражданским законодательством и законодательством об административных правонарушениях".

Защита информационных прав и свобод обеспечивается нормами институтов интеллектуальной собственности, института документированной информации, УК РФ, КоАП РФ, ГК РФ.

Примеры норм УК РФ: клевета (ст.129), оскорбление (ст.130), нарушение неприкосновенности частной жизни (ст.137), нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений (ст.138), отказ в предоставлении гражданину информации (ст.140), нарушение авторских и смежных прав (ст.146), отказ в предоставлении гражданину информации (ст.140), нарушение изобретательских и патентных прав (ст.147), воспрепятствование осуществлению права на свободу совести и вероисповеданий (ст.148), разглашение тайны усыновления (удочерения) (ст.155).

Примеры норм КоАП РФ: воспрепятствование осуществлению гражданином Российской Федерации своих избирательных прав либо работе избирательной комиссии; распространение ложных сведений о кандидате; нарушение прав члена избирательной комиссии (комиссии по проведению референдума), наблюдателя или иностранного (международного) наблюдателя; нарушение права граждан на ознакомление со списком избирателей"; нарушение условий проведения предвыборной агитации через средства массовой информации; изготовление или распространение анонимных агитационных материалов.

Примеры норм ГК РФ: компенсация морального вреда (ст.151), защита чести, достоинства и деловой репутации (ст.152).

Заключая рассмотрение правовых проблем информационной безопасности, отметим, что информационную безопасность можно рассматривать как аспект или ракурс изучения и формирования системы информационного права, подготовки и совершенствования норм и нормативных правовых актов этой отрасли. Используя результаты исследования в области информационной безопасности, законодатель и исследователь отрасли информационного права получают дополнительные возможности совершенствования средств и механизмов правовой защиты информационной безопасности в информационной сфере. Тем самым существенно повышаются качество и эффективность правового регулирования отношений в информационной сфере.

В этой связи структура правового регулирования отношений в области информационной безопасности как бы повторяет структуру самого информационного законодательства, акцентируя внимание на вопросах защищенности объектов правового регулирования, исходя из требований информационной безопасности. В итоге можно построить некоторую модель основных направлений защиты объектов информационной сферы и институтов информационного законодательства, с помощью нормативных предписаний которых решается проблема правового обеспечения защиты их информационной безопасности Правовое регулирование информационной безопасности формируется на базе информационных правоотношений, охватывающих все направления деятельности субъектов информационной сферы. Они охватывают все области информационной сферы, всех субъектов и объектов правоотношений.

Объекты правоотношений в области информационной безопасности - это духовность, нравственность и интеллектуальность личности и общества, права и свободы личности в информационной сфере; демократический строй, знания и духовные ценности общества; конституционный строй, суверенитет и территориальная целостность государства.

Субъектами правоотношений в области информационной безопасности выступают личность, государство, органы законодательной, исполнительной и судебных властей, система обеспечения безопасности, Совет Безопасности РФ, граждане.

Поведение субъектов в данной области определяются предписаниями законов и других нормативных правовых актов в порядке осуществления их прав и обязанностей, направленных на обеспечение защищенности объектов правоотношений.

Права и обязанности субъектов задаются нормами законов и иных нормативных правовых актов, устанавливающих правила поведения субъектов в порядке защиты объектов правоотношений, контроля и надзора за обеспечением информационной безопасности. Здесь же вводятся ограничения информационных прав и свобод в порядке защиты интересов граждан, общества, государства. При формировании норм права, установления прав и обязанностей применяются методы конституционного, административного и гражданского права.

Ответственность за правонарушения в информационной сфере устанавливается в порядке: защиты нравственности и духовности личности, общества, государства от воздействия недоброкачественной, ложной информации и дезинформации; защиты личности в условиях информатизации; защиты информации и информационных ресурсов от несанкционированного доступа (гражданско-правовая, административно-правовая, уголовно-правовая ответственность). Особенности установления ответственности за правонарушения в среде трансграничных информационных сетей, в том числе в Интернет основываются на особенностях и юридических свойствах информации, информационных технологий и средств их обеспечения.

Правовые механизмы защиты жизненно важных интересов личности, общества, государства должны разрабатываться и внедряться в каждой из областей информационной сферы.

1. Область поиска, получения и потребления информации.

Объекты правоотношений: духовность и нравственность гражданина, общества, государства (от воздействия недостоверной, ложной, вредной информации); информационные права и свободы человека и гражданина (право на получение и использование информации); честь и достоинство гражданина (в связи с созданием и распространением недостоверной информации или несанкционированным распространением личной информации о нем).

Субъекты правоотношений: человек и гражданин, потребитель информации, редакция.

2. Область создания (производство) исходной и производной информации.

Объекты правоотношений: информация как интеллектуальная собственность; документированная информация как интеллектуальная и вещная собственность.

Субъекты правоотношений: человек и гражданин, авторы, пользователи исключительных прав, издатели, потребители информации, органы государственной власти и местного самоуправления, органы и системы обеспечения защиты объектов информационной безопасности.

3. Область формирования информационных ресурсов, подготовки и предоставления пользователям информационных продуктов, информационных услуг.

Объекты правоотношений: право авторства и собственности на информационные ресурсы; информационные ресурсы на всех видах носителей, в том числе содержащие информацию ограниченного доступа.

Субъекты правоотношений: человек и гражданин, автор, пользователь, потребитель, участники самостоятельного оборота информации.

4. Область создания и применения информационных систем, технологий и средств их обеспечения.

Объекты правоотношений: автоматизированные информационные системы, базы и банки данных, другие информационные технологии, средства обеспечения этих объектов.

При этом, прежде всего, должны защищаться:

права авторов и собственников информационных систем и технологий, средств их обеспечения;

машинные носители с информацией, например, средствами электронной цифровой подписи; базы данных (знаний) в составе автоматизированных информационных систем и их сетей от несанкционированного доступа;

программные средства в составе ЭВМ, их сетей, информационные системы и их сети от несанкционированного доступа;

информационные технологии и средства их обеспечения.

Субъекты правоотношений: создатели, производители, заказчики, исполнители.

## Заключение

Цель курсовой работы достигнута, я осуществил целостно-логическое исследование состояния информационной безопасности в Российской Федерации.

По положениям, выносимым на защиту:

По первому положению: информационная безопасность общества, государства характеризуется степенью их защищенности и, следовательно, устойчивостью основных сфер жизнедеятельности экономики, науки, техносферы, сферы управления, военного дела, общественного сознания и.

Основой их защищенности должна стать законодательная основа защиты государственной тайны.

Правовая наука пока не может остановиться на какой-либо определенной модели в области регулирования и защиты интеллектуальной собственности и особенно исключительных прав создателей информационного и технологического продукта. Тем не менее, закон должен откликаться на коллизии в этой среде. Речь идет о том, что в процессе дополнений и изменений базового Закона и законов субъектов России необходимо уделить большее внимание означенным вопросам. Важное направление работы и области создания адекватной инфраструктуры в сфере информатики формируется вокруг создания и использования таких объектов, как информационные технологии и вычислительная техника.

По второму положению: информационная безопасность определяется способностью нейтрализовать воздействие по отношению к опасным, дестабилизирующим, деструктивным, ущемляющим интересы страны информационным воздействиям на уровне, как внедрения, так и извлечения информации.

В 2008 году только на сайт Президента Российской Федерации было осуществлено около 70 тысяч компьютерных атак. Всего же количество зарегистрированных атак на Интернет - представительства органов государственной власти Российской Федерации только в 2008 году превысило величину 630 тысяч. Все компьютерные атаки были успешно нейтрализованы средствами защиты сайтов, разработанными специалистами Центра.

ФСБ и ФСО сертифицировано 87 криптографических средств, предназначенных для защиты конфиденциальной информации, К настоящему времени у нас в стране только ФСБ и ФСО лицензировало порядка 300 организаций, которым дано право на разработку и производство средств криптографической защиты. Выдано 3500 лицензий на право распространения и эксплуатации криптографических средств защиты. При этом указанные лицензии получили организации, осуществляющие свою деятельность во всех экономически развитых регионах, и география лицензиатов охватывает всю территорию Российской Федерации.

В заключении необходимо сказать, что информационная безопасность России является базовой составляющей национальной безопасности России. Она напрямую влияет на эффективную работу органов государственной власти, является неотъемлемым фактором в борьбе с организованной преступностью и мировым терроризмом.

Излишняя открытость России в 90-х годах в период так называемой "демократизации" общества привела к крупным потерям, как в экономической, так и в политической составляющей Российской Федерации.

Внедрение современных технологий и законодательная основа защиты государственной тайны должна стать мощным звеном в укреплении вертикали власти в России и ее становлении как экономически и политически сильного государства на мировой арене.

## Список нормативных актов и литературы

Нормативные акты:

1. Конституция Российской Федерации М. Юридическая литература, 2003.

2. Федеральный закон от 21 июля 1993г. № 5485-1 "О государственной тайне", Федеральный закон от 06 октября 1997г. № 131-ФЗ "О внесении изменений и дополнений в Закон РФ "О государственной тайне".

3. Федеральный закон от 20 февраля 1995 г. № 24-ФЗ "Об информации, информатизации и защите информации" (принят государственной Думой 25 января 1995г).

4. Указ Президента РФ от 15 марта 2000г. № 511 "О Классификаторе правовых актов".

5. Указ Президента РФ от 16 декабря 1993 г. № 2171 "Об общеправовом классификаторе отраслей законодательства".

6. Указ Президента РФ от 12 мая 2004г. № 611 "О мерах по обеспечению информационной безопасности Российской Федерации в сфере международного информационного обмена".

7. Концепция национальной безопасности Российской Федерации (утверждена Указом Президента РФ от 17.12.1997 г. № 1300 (в редакции Указа Президента РФ от 10.01.2000г. № 24)).

8. Указ Президента РФ от 19 февраля 1999г. № 212 "Вопросы Государственной технической комиссии при Президенте Российской Федерации".

9. Положение о Государственной технической комиссии при Президенте Российской Федерации (утверждено Указом Президента РФ от 19 февраля 1999г. № 212).

10. Государственная программа обеспечения защиты государственной тайны в Российской Федерации на 1996-1997 годы (утверждена Указом Президента РФ от 9 марта 1996г. № 346).

11. Указ Президента РФ от 24 января 1998г. № 61 "О перечне сведений, отнесенных к государственной тайне".

12. Указ Президента РФ от 12 мая 2004 г. N 611 "О мерах по обеспечению информационной безопасности Российской Федерации в сфере международного информационного обмена"

13. Указ Президента РФ от 19 февраля 1999 г. N 212 "Вопросы Государственной технической комиссии при Президенте Российской Федерации"

14. Положение о Министерстве информационных технологий и связи Российской Федерации (утв. постановлением Правительства РФ от 26 июня 2004 г. N 311)

15. Приказ ФСБ РФ от 13 ноября 1999 г. N 564 "Об утверждении положений о системе сертификации средств защиты информации по требованиям безопасности для сведений, составляющих государственную тайну, и о ее знаках соответствия".

16. Приказ Гостелекома РФ от 21 июля 1999 г. N 22 "Об утверждении Положения о порядке, общих условиях и принципах использования на территории Российской Федерации систем глобальной подвижной персональной спутниковой связи (ГППСС) и требованиях по обеспечению информационной безопасности для российских сегментов указанных систем"

Периодическая печать

1. Никитов В.А. "Информатика в терминах и определениях российского законодательства" М. Юрист, 2006.

2. Горбачев В.С. Концептуальные вопросы применения средств криптографической защиты информации в информационных системах. М. 2007.

3. Тайна как элемент государственной безопасности (И.А. Слободанюк, "Российский военно-правовой сборник" N 1, апрель 2004 г.).

1. Декларация принципов "Построение информационного общества - глобальная задача в новом тысячелетии" от 12 декабря 2003 г. // Законодательство и практика масс-медиа. Вып. 1, январь 2004 г. [↑](#footnote-ref-1)
2. Окинавская Хартия глобального информационного общества от 22 июля 2000 г. // Дипломатический вестник. 2000. N 8. С. 51-56. [↑](#footnote-ref-2)
3. *Ожегов С.И.* Словарь русского языка. М., 1978. [↑](#footnote-ref-3)
4. См.: Советский энциклопедический словарь М.,1979. [↑](#footnote-ref-4)
5. Указ Президента РФ от 19 февраля 1999 г. N 212 "Вопросы Государственной технической комиссии при Президенте Российской Федерации" [↑](#footnote-ref-5)
6. Федеральный закон от 21 июля 1993г. № 5485-1 «О государственной тайне» [↑](#footnote-ref-6)
7. Федеральный закон от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации" // СЗ РФ. 2006. N 31 [↑](#footnote-ref-7)
8. Федеральный закон от 20 февраля 1995 г. № 24-ФЗ «Об информации, информатизации и защите информации» (принят государственной Думой 25 января 1995г.). [↑](#footnote-ref-8)
9. ВВС РФ. 1992. № 15. Ст. 779.1993. №2. Ст. 77; САПП РФ. 1993. №52. Ст. 5086. [↑](#footnote-ref-9)