

ОГЛАВЛЕНИЕ

Введение

Глава 1. Защита информации в Российской Федерации

1.1 Защита информации - приоритетная задача обеспечения национальной безопасности России

1.2 Практическое применение средств криптографической защиты в информационных системах

Глава 2. Законодательная база защиты информации в Российской Федерации

2.1 Нормативно-правовые основы защиты информации в Российской Федерации

2.2 Направления развития законодательства

2.3 Информационное законодательство - основной источник информационного права

2.4 Правовые проблемы информатизации экономики

Глава 3. Развитие информационного законодательства в Российской Федерации

3.1 Правовые категории информационного законодательства

3.2 Формирование политики информационного законодательства

Заключение

Список нормативных актов и литературы

ВВЕДЕНИЕ

Актуальность темы заключается в том, что потенциальные возможности развития основных сфер жизни общества и соответствующих компонентов обороноспособности определяются состоянием информационных процессов.

Кроме того, непосредственная актуальность темы определяется тем, что информационная безопасность на рубеже третьего тысячелетия выходит на первое место в системе национальной безопасности, формирование и проведение единой государственной политики в этой сфере требует приоритетного рассмотрения. Поскольку всякая политика в правовом государстве должна строиться на основе права, крайне важно определить такие правовые основы. Пока можно констатировать, что развитие общественных отношений в этой сфере существенно опережает развитие права по этим вопросам.

В настоящее время информация считается стратегическим национальным ресурсом - одним из основных богатств страны. Мировой объем производства информационной техники и информационных продуктов в конце 80-х годов превысил 500 млрд. долларов, а в настоящее время он превышает 2 трлн. долларов. В развитых странах это производство занимает первое место, как по объему, так и по числу занятых в нем людей. Под воздействием информатизации все сферы жизни общества (как и основная - экономическая) приобретают новые качества - гибкость, динамичность. Однако одновременно возрастает и потенциальная уязвимость общественных процессов от информационного воздействия. Международные эксперты по вопросам информатики считают, что на смену опасности возникновения ядерной катастрофы может прийти угроза развязывания войны, которая примет новые формы. Это будет

борьба, направленная против стран, обладающих передовой технологией, в целях создания хаоса в информационных структурах и порождения экономической катастрофы.

Впервые в России понятие «информационная безопасность» было введено в 1990 г. в парламентской комиссии академика Ю.А.Рыжова, которая занималась разработкой концепции национальной безопасности страны. С тех пор созданы соответствующие структуры в Правительстве РФ, в Администрации Президента РФ, в Совете безопасности РФ, которые

Объектом курсовой работы являются общественные отношения, складывающиеся в сфере информационной безопасности Российской Федерации.

Предметом курсовой работы являются нормативные правовые акты, регулирующие осуществление информационной безопасности в Российской Федерации.

Целью курсовой работы является целостно-логическое исследование состояния информационной безопасности в Российской Федерации.

В ходе своей работы выполнил следующие задачи:

- изучил и исследовал практическое применение средств криптографической защиты в информационных системах;
- описал и дополнил Нормативно-правовые основы защиты информации в Российской Федерации;
- систематизировал правовые категории информационного законодательства.

Исходя из поставленных задач, на защиту выносятся следующие основные положения курсовой работы:

1. Информационная безопасность общества, государства характеризуется степенью их защищенности и, следовательно, устойчивостью основных сфер жизнедеятельности (экономики, науки, техносферы, сферы управления, военного дела, общественного сознания и т.д.)
2. 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 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) Указ Президента РФ от 19 февраля 1999 г. N 212 "Вопросы Государственной технической комиссии при Президенте Российской Федерации".

В настоящее время большие изменения происходят в методологии защиты информации. Осуществляется переход от дорогостоящего скрывания заведомо завышенного объема данных к гарантированной защите принципиально важных, «узловых точек». Закладываются правовые основы такой деятельности. Приняты Закон Российской Федерации «О государственной тайне» Федеральный закон от 21 июля 1993г. № 5485-1 «О государственной тайне» и Федеральный закон «Об информации, информатизации и защите информации». 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. (6) Опубликование в открытой печати «Перечня сведений, отнесенных к государственной тайне» (7), открыло новый этап в обеспечении защиты информации, составляющей государственную тайну, явилось реальным результатом демократизации России в

части открытости и гласности.

1.2 Практическое применение средств криптографической защиты в информационных системах

В последнее время широкое распространение начинают получать системы электронной торговли, включая платежные системы (коммунальные платежи, услуги провайдеров, заказы продукции и т.д.), а также системы обмена электронными юридически значимыми документами (предоставление финансовой отчетности, налоговые декларации, заключение договоров и т.д.) при взаимодействиях между гражданами, фирмами, муниципальными и государственными органами. Вместе с тем, по мере развития технической информационной базы повышается и уязвимость информационного пространства. При этом на одно из первых мест встают вопросы обеспечения информационной безопасности при использовании открытых каналов передачи данных. Главной причиной этого является массовое использование для обработки информации средств вычислительной техники с программным обеспечением, позволяющим сравнительно легко модифицировать, копировать и разрушать обрабатываемую информацию, а также легкость доступа в современные открытые информационно-телекоммуникационные системы. Данное обстоятельство привело к тому, что в последнее время во всем мире, и в России в частности, резко растет число преступлений, связанных с применением компьютерной техники. Информационное пространство России включает в себя федеральный и региональный компоненты. Причем эти компоненты должны быть взаимосвязаны самым тесным образом и построены зачастую с использованием одинаковых или аналогичных технических средств. Отсюда с очевидностью следует, и об этом четко сказано в Доктрине информационной безопасности Российской Федерации, что задача обеспечения информационной безопасности этих компонентов может быть эффективно решена в рамках единой государственной политики, как на федеральном, так и на региональном уровнях.

Законодательством Российской Федерации, как и во многих передовых развитых странах, регулирование деятельности в области защиты информации отнесено к компетенции федеральных органов, среди которых можно выделить Гостехкомиссию и ФСБ России. В соответствии с проведенными в 2003г. мероприятиями по совершенствованию государственного управления в области безопасности Российской Федерации, регулирование деятельности в области защиты информации криптографическими методами отнесено к ведению ФСБ России (ранее эту функцию выполняло ФАПСИ). Названными выше организациями определяется порядок разработки и использования средств защиты информации, разрабатываются требования к средствам защиты в зависимости от важности защищаемой информации, сертифицируются разработанные средства защиты, выдаются лицензии на право разработки, производства и эксплуатации средств защиты. Принимая во внимание тот факт, что гражданам необходимы гарантии сохранения тайны их частной жизни, неприкосновенность имущества при осуществлении документированных операций с ним (например, операций с

банковскими вкладами), а также возможность получать достоверную информацию из государственных органов, применяемые технические средства защиты информации должны иметь достаточно высокие характеристики по надежности защиты информации. Применение криптографических методов и средств защиты информации при современном уровне развития криптографии и электронных технологий является, как правило, экономически более предпочтительным по сравнению с другими мерами защиты. Точнее, применение криптографических методов в комплексе с другими мерами является в ряде случаев обязательным условием надежной защиты перспективных информационно-телекоммуникационных технологий.

К настоящему времени отечественными предприятиями-разработчиками создан достаточно широкий спектр средств криптографической защиты информации, позволяющий обеспечивать защиту многих современных технологий обработки информации. Эти средства обеспечивают возможность защиты информации, обрабатываемой под управлением различных операционных систем и передаваемой по всевозможным каналам связи в соответствии с различными протоколами. ФСБ и ФСО сертифицировано 87 криптографических средств, предназначенных для защиты конфиденциальной информации. Необходимо отметить, что у нас в стране уже давно действует стандарт на криптографический алгоритм шифрования ГОСТ-28147, а также разработан и в 2001 году введен в действие новый стандарт ЭЦП ГОСТ Р 34.10-2001, по своим криптографическим свойствам не уступающий лучшим зарубежным стандартам. В 2004 году разработан межгосударственный стандарт ЭЦП стран СНГ ГОСТ 34.310-2004, который призван обеспечить защиту подлинности информации при организации защищенного документооборота с организациями и фирмами стран СНГ. К настоящему времени у нас в стране только ФСБ и ФАПСИ 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. Одним из важных аспектов обеспечения возможности организации информационного взаимодействия регионов на всех уровнях (внутрирегиональный, межрегиональный, связь регионов с Центром и т.п.) является проблема подключения к сети Internet в так называемом информационно безопасном варианте. Необходимо отметить, что 12 мая 2004 года Президент Российской Федерации подписал Указ № 611 «О мерах по обеспечению информационной безопасности Российской Федерации в сфере международного информационного обмена». В соответствии с этим Указом субъектам международного информационного обмена в Российской Федерации запрещается включение в состав средств международного информационного обмена, в том числе и в сеть «Интернет», информационных систем, сетей связи и автономных персональных компьютеров, в которых обрабатывается информация, содержащая сведения, составляющие государственную тайну, либо служебная информация

ограниченного распространения, а также запрещается подключать системы, для которых установлены особые правила доступа к информационным ресурсам. В качестве примера можно привести то обстоятельство, что в настоящее время создан и успешно функционирует Центр мониторинга, который обеспечивает оперативное обнаружение и установку источника компьютерных атак и вирусных заражений, направленных на информационные ресурсы органов государственной власти, включая и атаки, поступающие из сети Интернет. В 2003 году только на сайт Президента Российской Федерации было осуществлено около 100 тысяч компьютерных атак. Всего же количество зарегистрированных атак на Интернет - представительства органов государственной власти Российской Федерации только в 2003 году превысило величину 730 тысяч. Все компьютерные атаки были успешно нейтрализованы средствами защиты сайтов, разработанными специалистами Центра.

ГЛАВА 2. ЗАКОНОДАТЕЛЬНАЯ БАЗА ЗАЩИТЫ ИНФОРМАЦИИ В РОССИЙСКОЙ ФЕДЕРАЦИИ

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», 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 на 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 законодательства 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 использования 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 приходится 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 «закрывать» или «наказывать» - мало. В данном случае имеем в виду ситуацию, которая складывается в связи с новыми формами работы публичных библиотек, специальных информационных систем. Закрывать 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 законодательства. Информатика здесь дает новые инструментари, 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 уравниловка 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 по 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 отступления 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.

2.3 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 орган, 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.

2.4 Правовые проблемы информатизации экономики

В рассмотрении проблем информатизации экономики основное внимание уделяется на организацию использования результатов труда в рыночных формах. Даже решение этой задачи представляет немалую сложность. Оценка продукта программиста - программа, программное обеспечение информационной системы, причастность автора программы, с одной стороны, к получению вознаграждения за труд, а с другой - за прибыль в результате использования его продукта, пока не поддаются однозначному решению правовыми средствами. Наличие законов «О правовой охране программ для ЭВМ и баз данных», «О правовой охране топологий интегральных микросхем», принятых в 1992 г., не снимает всех проблем правового режима программной продукции, вопросов, связанных с гарантией прав авторов этого вида научно-технической продукции, защитой этих прав и реализации ответственности как автора, так и пользователей этим видом информационных технологий. Отнесение программ для ЭВМ к объектам авторского права при все увеличивающейся корпоративности производства и использования этого продукта приносит скорее моральное удовлетворение автору, который имеет право зарегистрировать свой продукт и таким образом закрепить свое авторство. Эти законы в связке с законом «Об авторском праве и смежных правах» устанавливают такие формы использования программ (и программного обеспечения - их совокупности), как адаптация; модификация; компилирование; воспроизведение; распространение (доступ любым, в том числе и сетевым, способом, путем продажи, проката, сдачи в наем, предоставления в займы, включая импорт для любой из этих целей); выпуск в свет, включение в хозяйственный оборот. Уже из этого перечисления способов использования программ видно, как переплетаются институты авторского и вещного права, насколько специфика этой части информационных технологий не укладывается в привычные рамки гражданско-правовых и авторских отношений.

Проблемы информационных технологий отражаются во всех конфликтных ситуациях современного решения прав субъектов на результаты интеллектуальной собственности и затрагивают вопрос о роли государства в обеспечении прав многих субъектов отношений в данной сфере. Это касается как непосредственных создателей данного продукта, так и прав собственников, на средства которых создается продукт, прав государства в этой области в том числе, пользователей продуктом.

Проблемы использования информационного ресурса в процессе их потребления разными социальными структурами тоже относятся к сфере государственно-правового регулирования. Это можно наблюдать на примере регулирования области массовой информации, распространения учебной, развлекательной информации; формирования сфер информационных услуг. Это наиболее шумная сфера технологий, ибо она представляет собой смешанную среду для информации машинной и обычной - бумажной, устной и т.п. Здесь формируется особая зона информационных угроз, усиливается острота проблем информационной безопасности.

Развитие доктрины информационного права имеет свою историю. Официально мысль о необходимости выделения такой отрасли права высказана еще в 1975. В настоящее время идея информационного права реализуется достаточно активно. За последние пять-семь лет сформирован большой массив российского законодательства и принято множество (несколько сотен) подзаконных актов, регулирующих разные направления деятельности в информационной сфере. В настоящее время многие проблемы решаются с учетом процессов формирования информационного общества.

Достаточно остро стоят вопросы развития международных норм в области информационных технологий и их использования. Концепция государственной информационной политики 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)., одобренная Государственной Думой и Постоянной палатой по государственной информационной политике Политического консультативного совета при Президенте РФ еще в 1998 г., предусматривала формирование «информационного права». Достаточно определено эти вопросы поставлены и в Доктрине информационной безопасности Российской Федерации 2000г Доктрина информационной безопасности Российской Федерации от 9 сентября 2000 г. N ПР-1895.

В настоящее время по уровню принятия нормативных правовых актов информационного законодательства и их действию и пространстве можно выделить федеральные акты, акты субъектов Российской Федерации и акты органов местного самоуправления.

Федеральный уровень источников информационного права представляется информационно-правовыми нормами Конституции РФ, федеральными конституционными законами, федеральными законами, указами и нормативными распоряжениями Президента РФ, постановлениями и нормативными распоряжениями Правительства РФ, нормативными правовыми актами федеральных министерств и ведомств:

- на уровне субъектов РФ - это законы и иные нормативные правовые акты высших органов государственной власти субъектов Российской Федерации и нормативные правовые акты органов исполнительной власти субъектов Российской Федерации.
- на уровне органов местного самоуправления представляются нормативными правовыми актами этих органов, принимаемыми в порядке применения норм

федерального уровня и уровня субъектов Российской Федерации.

Структура информационного законодательства может быть представлена следующей совокупностью информационных правовых норм и актов информационного законодательства:

- информационно-правовые нормы международных актов;
- информационно-правовые нормы Конституции РФ;
- нормативные правовые акты отрасли информационного законодательства;
- информационно-правовые нормы в составе других отраслей законодательства.

Полнота правового регулирования информационных отношений в информационной сфере может быть достигнута только в том случае, если совокупность информационно-правовых норм актов информационного законодательства «перекроет» все множество отношений матрицы информационных правоотношений применительно ко всем возможным объектам информационных правоотношений и субъектам, действующим в информационной сфере.

«Вертикальная» структура информационного законодательства, как и всего законодательства РФ, строится исходя из принципа верховенства закона: нормы вышестоящего по иерархии акта обладают более высокой юридической силой и, как правило, являются определяющими для соответствующих норм всех нижестоящих актов.

Наличие иерархии актов обусловлено тем, что на практике реализация правовых норм федерального закона нередко требует принятия правовых актов Президента РФ, Правительства РФ, актов субъектов Федерации, иных нижестоящих по иерархии актов. Система актов дополняется актами органов местного самоуправления, как бы исполняющих предписания норм вышестоящих актов в конкретных условиях.

Такая иерархия актов выстраивается с учетом распределения предметов ведения в информационной сфере Российской Федерацией и субъектов Российской Федерации (предметы ведения Российской Федерации, предметы совместного ведения Российской Федерации и субъектов Российской Федерации, предметы ведения субъектов Российской Федерации) в соответствии со ст. 71, 72 и 76 Конституцией РФ Конституция Российской Федерации М. Юридическая литература, 2003..

«Горизонталь» структуры информационного законодательства выстраивается исходя из того, что оно включает в свой состав не только нормы, входящие в блок специальных нормативных актов по институтам информационного права, но и нормы других отраслей законодательства РФ. Анализ зарубежного опыта и проведенные в России исследования в этом направлении лишней раз подтверждают, что информационное законодательство это комплексная отрасль, включающая как некоторые отрасли законодательства целиком и специальные нормативные акты, полностью посвященные проблемам информации, так и отдельные информационно-правовые нормы в актах других отраслей законодательства.

В целях унификации банков данных правовой информации, а также обеспечения автоматизированного обмена правовой информацией между федеральными органами государственной власти, органами государственной власти субъектов Российской Федерации, органами прокуратуры РФ и органами местного

самоуправления Указом Президента РФ от 15 марта 2000г. № 511 «О Классификаторе правовых актов» утвержден «Классификатор правовых актов» Указ Президента РФ от 15 марта 2000г. № 511 «О Классификаторе правовых актов»..