В.К. Сибирский

Правовая информатика

От автора

Отечественная правовая информатика имеет свою историю, традиции и опыт. Ее зарождение связывается с исследованиями многих авторов. Студенты приобретут немало полезных знаний, изучив и их труды. Необходимо также изучать законодательство иностранных государств в сфере правовой информатики. В учебно-методических материалах составлен достаточно подробный перечень нормативно-правовых источников и литературы по каждой из тем курса.

Изучение курса должно способствовать формированию и развитию у студентов высокой правовой культуры, пониманию международного права как самостоятельной комплексной отрасли национального права, умению применять как национальные, так и международные нормы, выработке способности и навыков работы в СПС российского права.

Изучение этого курса крайне важно для юристов и иных специалистов в области права и/или информатики, поскольку в современных экономических условиях особое внимание уделяется возникновению и установлению соответствующих правовых отношений с использованием информационно-телекоммуникационных технологий.

1. Информационное обеспечение правоохранительных органов

Информатизация государственной и правовой сферы России потребовала формирования новой разветвленной системы научных знаний. Этой потребности ответила новая междисциплинарная область знаний — правовая информатика.

Первоначально идеи общей и правовой информатики развивались в лоне кибернетики как науки о законах управления сложными динамическими системами. Лишь отдельные ученые ставили вопрос об информатике как самостоятельной науке. Так, один из ведущих специалистов данной сферы член-корреспондент АН СССР В.И. Сифоров выдвинул идею информологии — науки о законах передачи, распределения, обработки и преобразования информации. Информология должна была заняться кодированием, декодированием, запоминанием, хранением, поиском, извлечением, доставкой, сравнением, отображением, производством (генерированием), потреблением информации.

Термин «информатика» возник в 60-х гг. во Франции для названия области автоматизированной обработки информации с помощью электронных вычислительных машин. Французский термин informatique образован путем слияния слов information (информация) и automatique (автоматика) и означает «информационная автоматика», «или автоматизированная переработка информации». В англоязычных странах этому термину соответствует computer science (наука о компьютерной технике).

В конце 60-х гг. понятие «информатика» связывалось в нашей стране не только с информационной техникой, но и с теорией научной информации («документалистикой»). Этому во многом способствовал выход труда А.И. Михайлова, А.И. Черного и Р.С. Гиляровского «Основы информатики». В работе были подробно рассмотрены понятия научно–технической информации и методы ее обработки. В 1982 г. вышла в свет монография выдающегося ученого в области кибернетики и

информатики лауреата Ленинской премии академика АН СССР В.М. Глушкова «Основы безбумажной информатики». В монографии были рассмотрены понятие информации и методы ее обработки (справочные системы, преобразование информации, языки для описания данных, телекоммуникационные системы), практические вопросы безбумажных технологий в сфере научных исследований, редакционно–издательской деятельности, в медицине, обучении, проектных работах, кредитно–финансовых отношениях. Особое внимание уделено автоматизации организационных систем и смежным вопросам. Выдвинута идея ОГАС.

Значительную роль в становлении понятийного аппарата информатики сыграла монография Г.Р. Громова «Национальные информационные ресурсы: проблема промышленной эксплуатации». В ней рассмотрены такие вопросы, как понятие национальных информационных ресурсов, их промышленная эксплуатация, темпы роста индустрии ЭВМ, перспективы развития информационных технологий и науки программирования. Информационные ресурсы — непосредственный продукт интеллектуальной деятельности наиболее квалифицированной и творчески активной части трудоспособного населения страны. Национальные информационные ресурсы — относительно новая экономическая категория. Корректная постановка вопроса о количественной оценке этих ресурсов и их связи с другими экономическими категориями требуют длительных совместных усилий специалистов и ученых самых разных областей знаний.

У нас современная трактовка термина «информатика» утвердилась с момента принятия решения в 1983 г. на сессии годичного собрания Академии наук СССР об организации Отделения информатики, вычислительной техники и автоматизации. Информатика практиковалась как «комплексная научная и инженерная дисциплина, изучающая все аспекты разработки, проектирования, создания, оценки, функционирования основанных на ЭВМ систем обработки информации, их применения и воздействия на различные области социальной практики».

С конца 80-х гг. в СССР начинается вторая компьютерная революция. Термин «информатика» обозначает теперь не только науку, но и направление практической деятельности. Информатика как отрасль народного хозяйства состоит из однородной совокупности предприятий разных форм хозяйствования, связанных с производством компьютерной техники, программных продуктов и разработкой современной технологии переработки информации.

Существует разветвленная система наук, предметом которых являются информация и информационные процессы. Это и теоретическая информатика, изучающая общие закономерности информационных процессов и их математические модели; и социальная информатика, изучающая особенности информационных процессов в обществе; и прикладная информатика, ориентированная на применение средств автоматизации для решения прямых практических задач; и отраслевые направления информатики, изучающие информационные процессы в конкретных науках (экономика, социология, право и др.).

Современная информатика сложилась в недрах математики и кибернетики, системотехники и электроники, логики и лингвистики. Ее основные научные направления образуют такие дисциплины, как теоретические основы вычислительной техники, статистическая теория информации, программирование и искусственный интеллект. Технические и программные средства информатики все шире используются в современной юридической практике, в деятельности органов правоохраны и правопорядка; в системах сбора, хранения, передачи, обработки, выдачи управляющей и осведомляющей правовой информации с использованием компьютеров, компьютерных сетей и телекоммуникаций, связывающих в единый комплекс отдельные компьютеры на сколь угодно большой территории.

Информатика как прикладная дисциплина занимается:

изучением закономерностей в информационных процессах (накопление, переработка, распространение информации);

созданием информационных моделей коммуникаций в различных областях человеческой деятельности;

разработкой информационных систем и технологий.

Правовая информатика представляет собой прикладную ветвь общей информатики. Существуют различные подходы к пониманию задач и природы правовой информатики. С учетом высказанных точек зрения можно дать следующее определение. Правовая информатика — это междисциплинарная отрасль знания о закономерностях и особенностях информационных процессов в сфере юридической деятельности, об их автоматизации, о принципах построения и методиках использования автоматизированных информационных систем, создаваемых для совершенствования и повышения эффективности юридической деятельности и решения правовых задач на базе комплексного использования теории и методологии правовых наук, средств и методов математики, информатики и логики.

В задачи правовой информатики входят:

активное участие в создании правового государства на принципах плюралистической демократии и гласности, доступности для каждого члена общества всей совокупности нормативных правовых актов, свободного получения информации в нужное время, в нужном месте и в нужной форме;

разработка научных и практических основ внедрения автоматизированных рабочих мест (АРМ), интеллектуальных и консультационных систем;

интеллектуализация деятельности юридических учреждений и органов, повышение производительности труда и культуры в отправлении правосудия и других форм юридической работы;

создание автоматизированных обучающих систем; разработка теоретических и методических проблем подготовки и переподготовки юридических кадров, формирование корпуса молодых специалистов по новой юридической специальности — «правовая информатика».

В настоящее время правовую информатику можно рассматривать как перспективное и быстро прогрессирующее направление научных исследований, которое имеет собственный предмет, задачи и методы исследований. Восприятие юристами положений и выводов информатики должно происходить через призму юридических понятий и категорий.

Несмотря на короткий срок своего существования, правовая информатика добилась существенных несомненных успехов в реализации государственной политики информатизации правовой сферы России. К ним относятся:

создание сети центров и всероссийских систем правовой информации;

формирование законодательства об информации и информатизации;

создание системы знаний;

введение курсов математики и информатики;

выход на международный уровень.

Как и многие другие отрасли знания, правовая информатика делится на общую и специальную части.

Общая часть включает:

задачи создания Общенациональной системы правовой информации;

государственную политику информатизации правовой, государственной и политической системы;

понятие единого информационного пространства;

понятие общей и правовой информации;

методологию и методы исследования.

Особенная часть правовой информатики исследует пути и задачи применения компьютерных технологий в различных сферах и направлениях государственно–правового регулирования общественных отношений: в правотворческой и правоприменительной деятельности, в

криминалистике и судебной экспертизе, в социологических исследованиях.

Постепенно происходит уточнение научного статуса и профиля правовой информатики. Правовая информатика не сложилась еще в самостоятельную науку. По шкале оценок она занимает более низкий ранг, а именно — ранг междисциплинарной отрасли знания.

Правовую информатику необходимо отличать от ряда смежных научных направлений, что, однако, не снижает ее научной и практической значимости. Так, правовую информатику необходимо отграничивать от курса «Информационное право». В задачи этого курса входит изучение законодательства об информации и информатизации. Самостоятельная информационная дисциплина — «Курс компьютерной грамотности» введен в число учебных дисциплин средней школы и преподается во всех вузах страны, включая юридические.

Государственная информационная политика — это часть внутренней и внешней политики государства, которая состоит в регулировании информационных потоков и информационной деятельности различных государственных, общественных, частных структур и организаций информационного профиля. В России законодательной базой в области правового регулирования информации служат Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» и изданные на его основе иные нормативные правовые акты, в соответствии с которыми основными направлениями государственной политики в сфере информатизации являются:

обеспечение условий для развития и защиты всех форм собственности на информационные ресурсы;

формирование и защита государственных информационных ресурсов;

создание и развитие федеральных и региональных информационных систем и сетей, обеспечение их совместимости и взаимодействия в едином информационном пространстве Российской Федерации;

создание условий для качественного и эффективного информационного обеспечения граждан, органов государственной власти, органов местного самоуправления, организаций и общественных объединений на основе государственных информационных ресурсов;

обеспечение национальной безопасности в сфере информатизации, а также обеспечение реализации прав граждан, организаций в условиях информатизации;

содействие формированию рынка информационных ресурсов, услуг, информационных систем, технологий, средств их обеспечения;

формирование и осуществление единой научно-технической и промышленной политики в сфере информатизации с учетом современного мирового уровня развития информационных технологий;

поддержка проектов и программ информатизации;

создание и совершенствование системы привлечения инвестиций и механизма стимулирования разработки и реализации проектов информатизации;

развитие законодательства в сфере информационных процессов, информатизации и защиты информации.

Итак, в России информатизация правовой сферы жизни общества поднята до уровня государственной политики. Государство при участии негосударственных структур проводит целенаправленный комплекс мер по внедрению в деятельность органов власти и управления новейших информационных технологий, компьютерных систем и сетей, автоматизированных рабочих мест, экспертных и консультационных систем (на базе идей искусственного интеллекта).

Государственная политика информатизации правовой сферы имеет своей конечной целью создание в России общенациональной автоматизированной системы правовой информации, посредством чего должна быть обеспечена более полная правовая информированность граждан, повышение эффективности права и его применения, и тем самым усилена «правовая плотность общества». Она призвана охватить территорию всей России, все регионы и поднять на более высокий уровень деятельность органов государственной власти и управления,

правоохранительных органов, органов местного самоуправления. Как показывают расчеты, в некоторых областях юридической деятельности информатизация позволяет увеличить производительность труда юристов в несколько раз.

Нормативной основой информатизации правовой сферы является ряд указов Президента РФ. Указ Президента РФ от 28 июня 1993 г. № 966 «Концепция правовой информатизации России» определяет основные направления информатизации:

информатизация правотворчества;

информатизация правоприменительной деятельности;

информатизация правоохранительной деятельности;

информатизация правового образования и воспитания;

правовое обеспечение процессов информатизации.

Однако этот Указ не решил всех проблем нормативно-правового регулирования данной сферы. В нем в минимальной мере затронуты организационно-правовые вопросы. Этот пробел был восполнен Указом Президента от 4 августа 1995г. «О президентских программах по правовой информатизации». Данным указом предусмотрена разработка программ правовой информатизации:

органов государственной власти РФ;

органов исполнительной власти РФ;

органов государственной власти субъектов РФ.

Информатизация влияет не только на эффективность юридических технологий, сферу правотворчества и право реализации, но и на существо правовых отношений. Все большую роль играют такие понятия, как электронная сделка, электронное издание, электронная биржа, электронные торги, электронная система финансовых расчетов, электронный архив и т.п.

Информация в правоохранительных органах состоит из данных о:

владельцах моторизованных средств передвижения (к которым относятся автомобили, вертолеты, катера, мотоциклы, мотороллеры, самолеты, яхты и др.),

владельцах огнестрельного оружия,

похищенных предметах (вещах),

правонарушениях,

преступниках и правонарушителях,

прописке (и регистрации для Москвы).

Учет — это система регистрации и хранения информации о лицах, совершивших преступления, о самих преступлениях и связанных с ними фактах и предметах. Он занимает основное место в информационном обеспечении правоохранительных органов. Совокупный объем учетов органов МВД Российской Федерации охватывает около 95% криминальных проявлений, с их использованием удается раскрывать до 25% преступлений. Самый крупный центр хранения информации в России — Главный Информационный Центр Министерства внутренних дел Российской Федерации (ГИЦ МВД РФ). Он содержит свыше 100 миллионов учетных документов и имеет картотеку осужденных лиц, фототеку отпечатков пальцев, подробные отчеты органов милиции. Имеются также региональные Информационные Центры МВД и информационные Центры Управлений внутренних дел (УВД), которые также содержат обширную информацию, включая оперативную, оперативно-розыскную, криминалистическую и др.

Помимо учетов, в органах МВД создаются и хранятся экспертно-криминалистические централизованные коллекции и картотеки, предназначенные для раскрытия и расследования преступлений. Информация в учетах, коллекциях и картотеках называется криминальной.

По своим функциям учеты делятся на:

оперативно-справочные;

розыскные;

криминалистические;

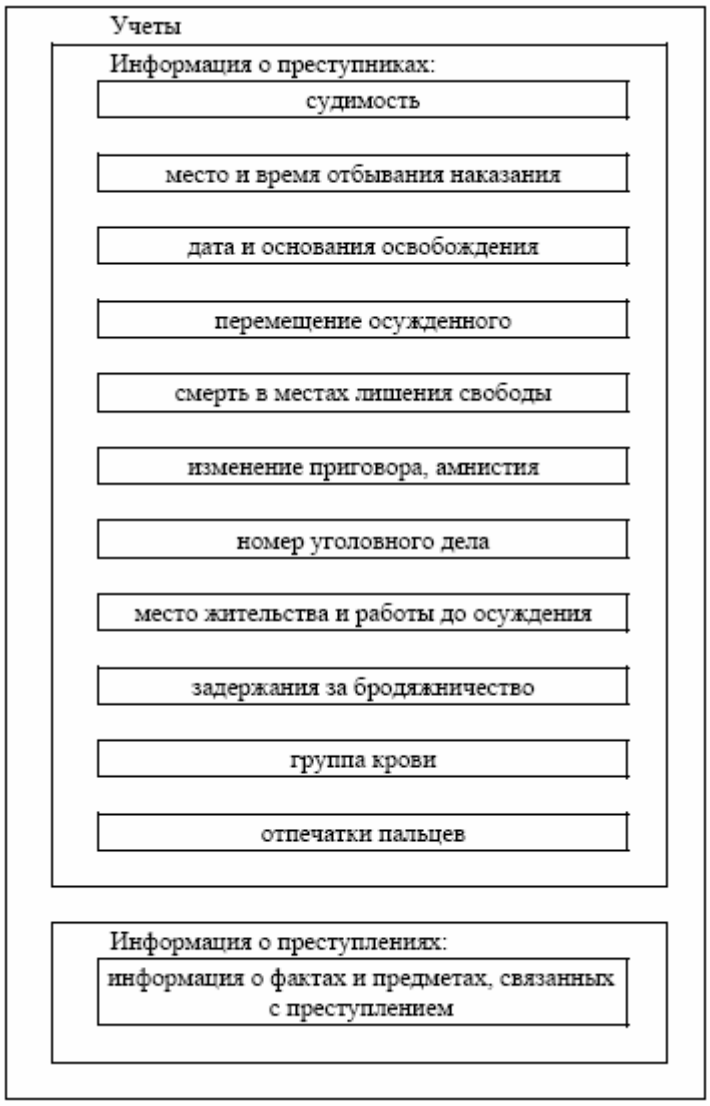
а по объектам на:

лица;

преступления;

предметы.

Учеты содержат следующие сведения о гражданах России, иностранцах и лицах без гражданства (рис. 1.1).



По отпечаткам пальцев можно устанавливать личности преступников, арестованных, задержанных, трупов, неизвестных больных. В информационных центрах имеется около 30 миллионов отпечатков пальцев, и они обслуживают свыше миллиона запросов органов внутренних дел (ОВД) в год. Надо отметить, что во многих развитых странах введено снятие (при отсутствии) и регистрация отпечатков со всех лиц пребывающих на территории страны. С этим связана необходимость использования биометрических паспортов.

По способам обработки информации бывают ручные, механизированные и автоматизированные учеты. Автоматизированные учеты представляют собой ряд автоматизированных информационно-

поисковых систем (АИПС), работающих, в основном, по принципу «запрос-ответ». Имеются, например, АИПС:

«Картотека»;

«Опознание»;

«Оповещение» (розыск по искам предприятий);

«Оружие»;

«Автопоиск» (розыск автомашин);

«Антиквариат»;

«Вещь» (похищенные номерные вещи);

«Сейф» (преступления со взломом сейфов);

«Досье» (рецидивисты, особо опасные преступники);

«Насилие» (преступления с насилием против личности).

Для иностранцев и лиц без гражданства есть специальная АИПС «Криминал-И». В МВД имеется также сеть автоматизированных банков данных (АБД), объединяющая множество локальных вычислительных сетей и других информационных систем, а также множество автоматизированных рабочих мест (АРМ).

Для использования криминальной информации в полном объеме необходима автоматизированная информационно-поисковая система (АИПС), называемая системой криминалистической регистрации (табл. 1.1). В нее входит ряд подсистем по различным видам учетов.

Таблица 1.1.

Система криминалистической регистрации

Система хранения и поиска криминальной информации				
Федеральный Банк Криминальной Информации		***Региональные Банки Криминальной Информации***		
АИПС «Картотека»	АИПС «Опознание»	АИПС «Оповещение»	АИПС «Оружие»	АИПС «Автопоиск»
АИПС «Антиквариат»	АИПС «Вещь»	АИПС «Сейф»	АИПС «Досье»	АИПС «Насилие»
АИПС «Криминал-И»	АИПС «Документ»	АИПС «Гильза»	АДИС	АБД
	ЛВС		ЛВС	
АРМ	АРМ	АРМ	АРМ	АРМ

Оперативно-справочные учеты накапливаются в Главном Информационном Центре (ГИЦ) МВД, в Федеральном Банке Криминальной Информации (ФБКИ), в Региональных Банках

Криминальной Информации (РБКИ) и в других информационных центрах. Они составляют единую сеть — Информационно-вычислительную сеть (ИВС) ОВД. Для особо опасных преступлений имеется система «Досье», связанная с централизованной фототекой и видеотекой. Отметим следующие АИС и АИПС.

Автоматизированная дактилоскопическая информационная система (АДИС) — для дактилоскопической регистрации. Для ввода изображений (дактилокарт) используются сканеры и телекамеры. АДИС позволяет находить пары совпадающих изображений (введенного и хранимого), причем процент правильно найденных пар составляет 70—95%. Могут выдаваться и недостаточно идентифицированные пары для ручного просмотра. Имеется несколько успешно функционирующих АДИС. Так, например, АДИС«Папилон» отечественной разработки предназначена для сравнения дактилокарт; АДИС «Узор» — картотека отпечатков с мест нераскрытых преступлений («следотека»). Существуют и более мощные АДИС.

АИПС «Криминал-И» — для учета правонарушений и преступлений, совершенных иностранцами, лицами без гражданства и гражданами России, постоянно проживающими за границей.

АИПС «Антиквариат» — учет похищенных предметов антиквариата и культурных ценностей.

АИПС «Номерная вещь» — учет похищенных номерных вещей.

АИПС «Документ» — учет похищенных документов общегосударственного обращения.

АИПС «Автопоиск» и «Розыск» — учет похищенного автотранспорта.

Имеется система автоматизированных банков данных по правовым делам, обслуживающая запросы четырех типов: на учетное лицо, на преступление, на вещь, на оружие. Система является универсальной, но учитывает мало типов криминальной информации. Для узкого круга задач имеются специализированные криминалистические АИПС, например, для учета гильз («Гильза»), для дел с сейфами («Сейф») и некоторые другие.

Информационной базой статистического анализа преступности является государственная уголовная статистика (учет преступлений, преступников, уголовных дел). Первичный учет ведут ОВД; учитывается около 95% криминальных проявлений. Выявляются состояние, уровень, состав, структура преступности; причины и условия преступлений, личности преступников; изучается система борьбы с преступностью. Требуется четкая система сбора информации о преступности и результатах борьбы с ней; это весьма трудоемкая работа. Имеются государственная и ведомственные статистические отчетности. Необходим единый учет всех преступлений на основе документов первичного учета, допускается безбумажная технология с использованием компьютеров.

Первичный учет состоит в заполнении статистических карточек на преступление, результаты расследования, лиц (подозреваемых в совершении преступления), движение уголовного дела, изъятие предметов преступной деятельности, результаты возмещения ущерба, результаты рассмотрения в суде. Эти первичные учеты регистрируются в местных ОВД и направляются в информационные центры МВД. В информационных центрах ведутся журналы учета преступников, лиц, дел; формируется статистическая отчетность о преступности, проводится статистический анализ (обнаружение взаимосвязей криминальных явлений, их эволюция), вычисляются обобщающие показатели. Основные направления в уголовной статистике — это усовершенствование системы статистических показателей, автоматизация сбора и обработки статистической информации, использование современных математических методов для ее анализа.

Имеются четыре формы государственной отчетности:

1) отчет о преступлениях (зарегистрированных, раскрытых и нераскрытых);

2) отчет о лицах, совершивших преступления;

3) отчет о преступности;

4) отчет о следственной работе.

Имеется также много форм ведомственной отчетности и форм об оперативно-служебной деятельности.

Основными задачами учетно-регистрационной и статистической работы являются:

1) регистрация и учет преступлений и правонарушений; лиц, материалов дел, протоколов;

2) сверки учетных данных со статистическими данными Информационного центра МВД, Главного управления внутренних дел, Управлений внутренних дел, Управления внутренних дел на транспорте;

3) контроль полноты и своевременности регистрации криминальной информации в местных отделениях;

4) контроль своевременности представления документов первичного учета в вышестоящие органы;

5) контроль полноты и объективности документов первичного учета;

6) формирование статистических отчетов;

7) подготовка справочных материалов для руководящих органов.

Для эффективного использования компьютерных технологий в криминальной статистике необходимы мощные технические и программные средства.

2. Информационно-телекоммуникационные технологии правоохранительной деятельности

Под информационно-телекоммуникационными технологиями здесь будем понимать систему операций по сбору, хранению, обработке и передаче правоохранительной информации с помощью компьютеров. Эти технологии используются для обработки криминальной информации, управления, автоматизации офисных работ, принятия решений, функционирования экспертных систем. Средства информационно-телекоммуникационных технологий обычно включают электронную почту, аудиопочту, текстовые процессоры, электронные таблицы, телеконференции, видеотекст и др. Широко используются средства мультимедиа, к которым относятся неподвижные изображения на экране в сочетании со звуковыми эффектами, движущиеся изображения, анимация (аналог мультипликации).

В органах внутренних дел имеется Федеральный банк криминальной информации. Для усиления этой базы требуются мощные компьютеры с соответствующими программными средствами и мощными СУБД, например типа Oracle, способными обеспечить многопользовательский, многозадачный режим работы компьютерной сети. Использование таких операционных систем, как Unix или Windows также может давать хорошую защиту информации при одновременной работе многих пользователей. Для автоматизированных рабочих мест хорошо зарекомендовали себя СУБД «Paradox», «Clipper», пакет прикладных программ (ППП) «Flint».

Помимо Федерального банка криминальной информации, расширяется сеть региональных информационных центров, связанных с Главным информационным центром. Уже в настоящее время в этой сети ежегодно обрабатывается свыше 200 миллионов правовых документов.

В правоохранительной деятельности по своему назначению можно выделить автоматизированные информационные системы (АИС) для сбора и обработки учетной и статистической информации, оперативные, для следственной практики, криминалистические, управленческие, для

экспертной деятельности. Используются автоматизированные системы обработки данных (АСОД), автоматизированные информационно-поисковые системы (АИПС), автоматизированные информационно-справочные системы (АИСС), автоматизированные рабочие места (АРМ), автоматизированные системы управления (АСУ), экспертные системы. Возможны и комбинации этих АИС (табл. 2.1).

Таблица 2.1.

Автоматизированные информационные системы правоохранительной деятельности

Правовые автоматизированные информационные системы						
АИС	*АСОД*	*АИСС*	*АИПС*	*АРМ*	*АСУ*	*Экспертные системы*
для сбора и обработки учетной и статистической информации		«Сводка»				
оперативные		«Гастролеры»				
для следственной практики		«Грузы-ЖД»				
криминалистические		«Наркобизнес»				
управленческие		«Картотека-Регион»				
для экспертной деятельности		«Спецаппарат»				

АСОД обычно применяются для выполнения относительно несложных, стандартных операций с данными, автоматизируют работу персонала невысокой квалификации. АИПС служат для поиска, отбора, выдачи правовой и криминалистической информации по запросам, оформленным соответствующим образом; бывают документальные и фактографические. АИСС выдают справки по вопросам правоохраны и правопорядка по запросам без сложного преобразования данных.

АИСС «Сводка» выдает справки о происшествиях, преступлениях по оперативной информации.

АИСС «Гастролеры» выдает справки о преступлениях на транспорте, неразысканных вещах, подозрительных лицах и их связях; с использованием ППП «Flint» может решать поисковые задачи типа «лицо», «нераскрытые преступления», «вещи».

АИСС «Грузы-ЖД» снабжает справками о хищениях груза и багажа на железных дорогах.

АИСС «Наркобизнес» предоставляет справки по криминальному обороту наркотиков.

АИСС «Картотека-Регион» с использованием СУБД «Adabas» выдает фамилии, имена, отчества осужденных, разыскиваемых лиц, бродяг, задержанных; может распределять места отбытия наказания, решать административные задачи по осужденным лицам.

АИСС «Спецаппарат» предназначена для работы со спецаппаратом и поиска информации по спецсообщениям (поиск лиц по однотипным преступлениям и способам совершения, по адресам и т.п.).

Автоматизированное рабочее место (АРМ) представляет собой комплекс технических и программных средств автоматизации профессиональной деятельности. В типовой состав АРМ входят:

персональный компьютер;

принтер;

плоттер;

сканер;

факс;

средства сетевой связи

и другие устройства, а из программных средств:

текстовый процессор;

электронные таблицы;

графические процессоры;

офисные приложения.

Под АРМ иногда понимают рабочие места, а иногда — ППП. Существуют три типа АРМ:

1) индивидуального пользования;

2) группового пользования;

3) сетевые.

Сетевые АРМ наиболее перспективны, так как позволяют связываться с удаленными банками данных и обмениваться информацией между различными подразделениями правоохранительных

органов. Примером может служить АРМ «ГРОВД» для городских и районных отделов внутренних дел.

АСУ представляют собой комплексы технических и программных средств для автоматизированного управления различными службами и органами правоохраны. Основная функция таких АСУ — обеспечение руководителей служебной информацией. Практически это система связанных АРМ. Примером может служить АСУ «Дежурная часть» (АСУ ДЧ), предназначенная для управления силами и средствами ОВД в оперативной работе.

Основные функции АСУ:

1) оперативный сбор и анализ оперативной информации, выдача указаний подразделениям ОВД, контроль выполнения оперативной работы в реальном масштабе времени, управление подвижными милицейскими группами (на автомобилях, мотоциклах и других моторизованных средствах передвижения);

2) сбор, обработка, хранение информации; отображение информации о размещении сил и средств, а также о местах совершения преступлений на фоне представленных на экране («электронных») карт;

3) сбор информации о правонарушителях, похищенных вещах и транспортных средствах; выдача информации по запросам органов внутренних дел с использованием банков данных;

4) регистрация деятельности органов внутренних дел, подготовка отчетов о работе, анализ процессов (событий).

Использование АСУ позволяет радикально упростить и ускорить выполнение указанных работ. При раскрытии и расследовании преступлений может использоваться как универсальное, так и специальное программное обеспечение. К широко используемому универсальному программному обеспечению АСУ относятся:

1) текстовые процессоры для написания и редактирования текстов. Наиболее распространен сейчас текстовый процессор «MS Word». Текстовый процессор позволяет редактировать готовый текст, монтировать документы из фрагментов, корректировать орфографию,

помещать в текст рисунки, готовить цветные документы, выполнять многие другие действия. Поскольку документы сохраняются в памяти компьютера, их можно повторно использовать;

2) системы редактирования изображений — для подготовки иллюстраций к протоколам и другим документам. Наиболее широкое распространение в юридической практике получили графические процессоры «Adobe Photoshop», «Corel Draw» и некоторые другие;

3) программное управление базами данных — для переработки и систематизации однотипных данных, выборки необходимых данных и т.п. Можно создавать электронные записные книжки или картотеки, в которые можно вносить, редактировать, сохранять или исключать данные; создавать электронный график работы и получать напоминание о текущих делах (например, с использованием программ «Binder» или «Outlook»);

4) электронные таблицы. Для работы с таблицами особенно часто используется табличный процессор «Excel», включенный в пакет прикладных программ «MS Office»;

5) программы распознавания текстов, вводимых со сканеров, например, программа «FineReader». Использование сканеров значительно ускоряет подготовку различных правовых документов;

6) программы перевода служебных и официальных документов с русского языка на другие языки (английский, французский, немецкий, украинский) и наоборот. Наиболее распространенной для этих целей является программа «Promt»;

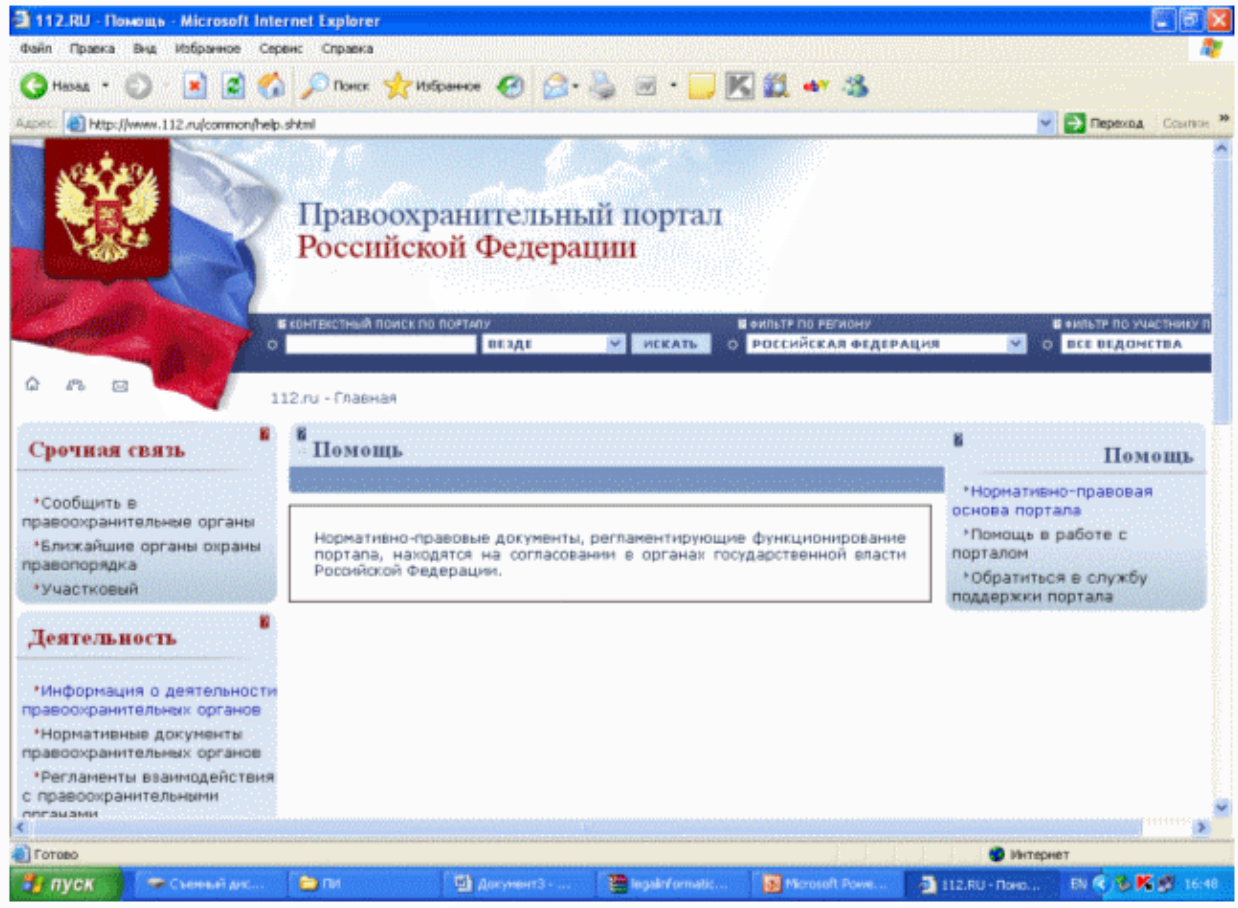
7) программы для работы в сети «Интернет», включая работу с электронной почтой. Наиболее распространенной для этих целей является программа «Internet Explorer», также входящая в офисные приложения «MS Office».

Использование указанного ПО значительно ускоряет и облегчает труд следователя по составлению, рассылке, упорядочению многочисленных служебных документов (запросов, справок, отчетов, распоряжений, планов, постановлений, заключений), который занимает

значительную часть его времени и очень замедляет расследование, что крайне нежелательно.

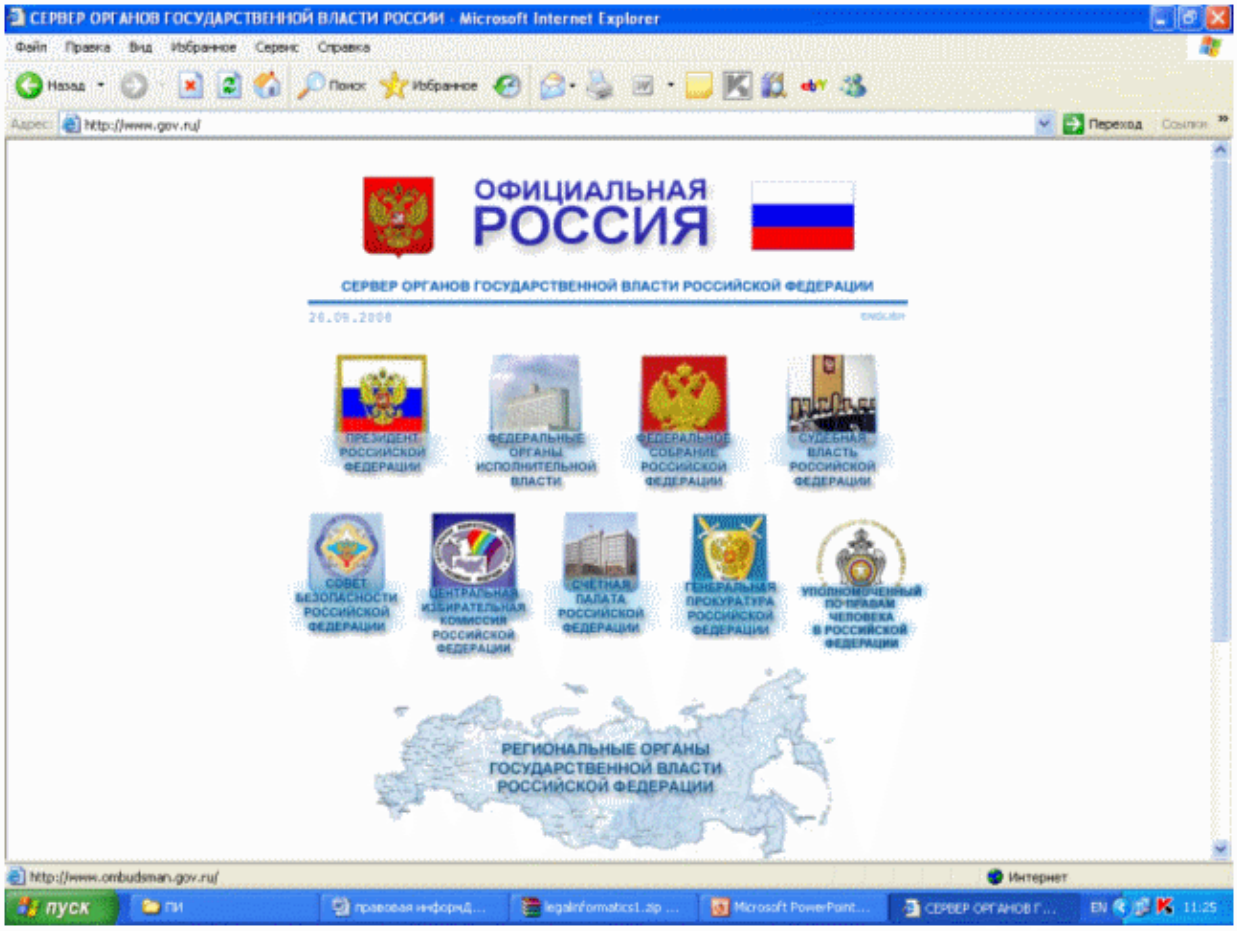
Отметим здесь несколько Интернет-ресурсов РФ в области правовой информатики.

Специализированная информационно-справочная система (СИСС) «Правоохранительный портал Российской Федерации» (рис. 2.1).

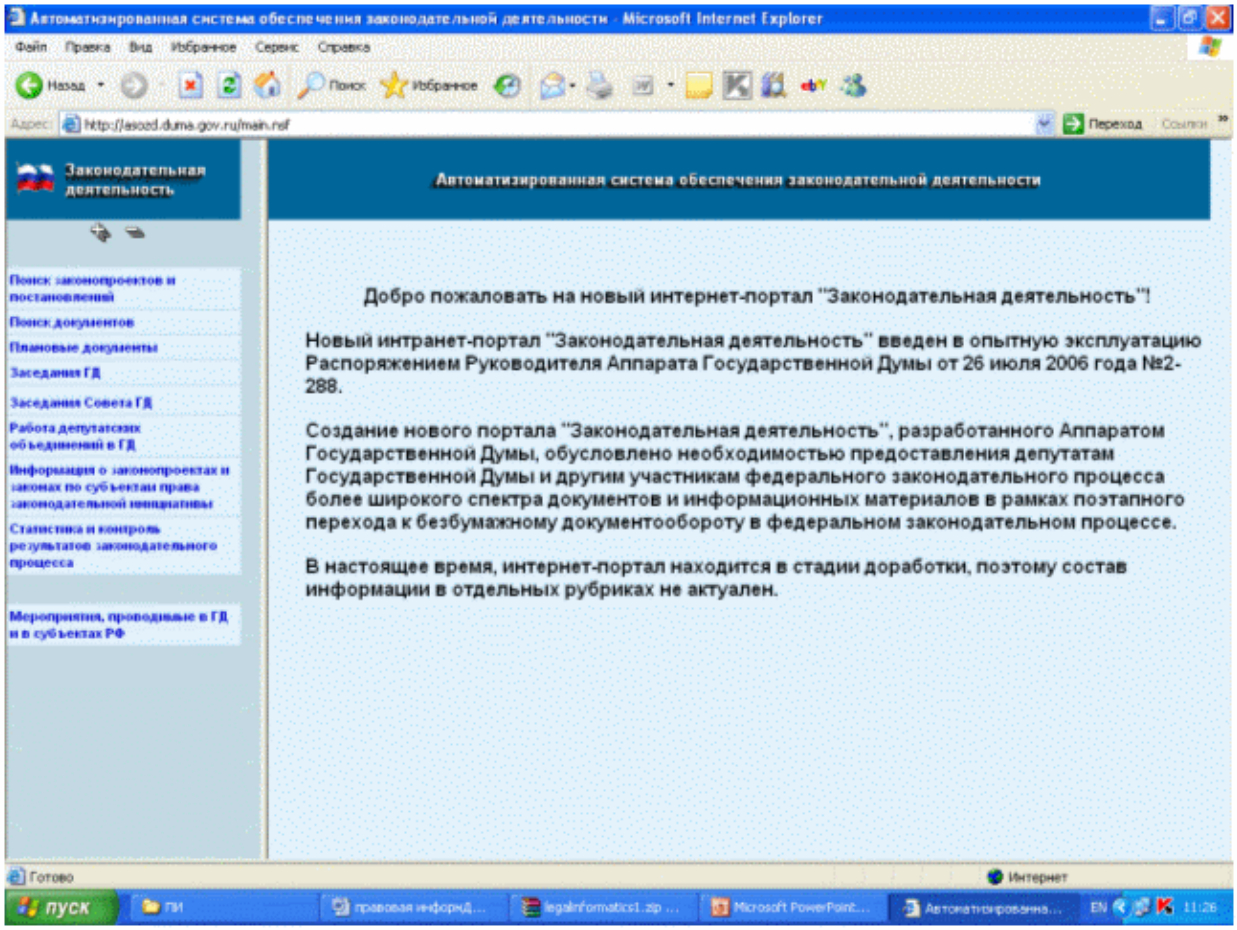


Система введена в эксплуатацию в начале 2009г. согласно Распоряжению Правительства РФ от 10 января 2009 года № 16-р. МВД России определено ответственным за организационное обеспечение функционирование системы.

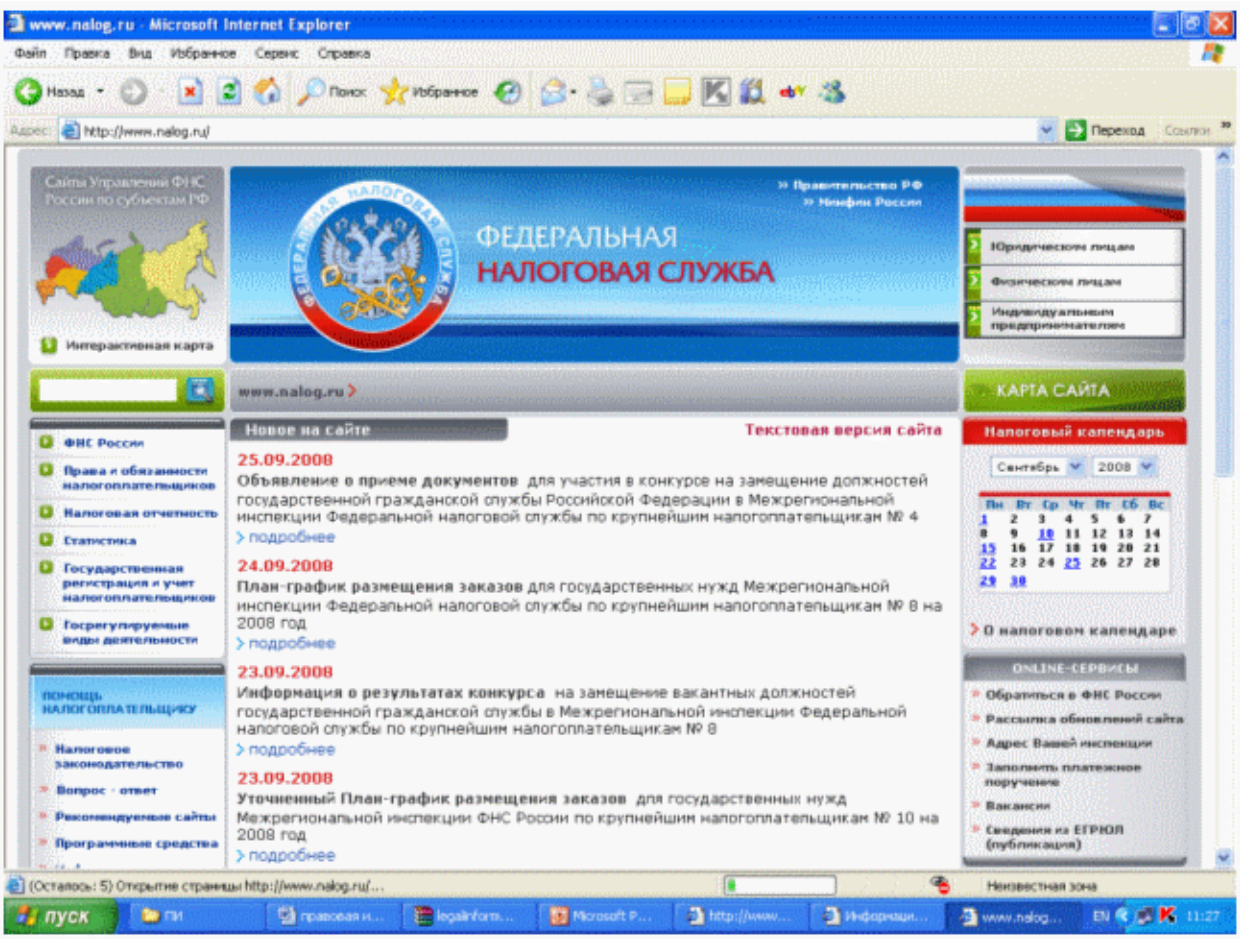
Портал федеральных органов государственной власти (рис. 2.2).



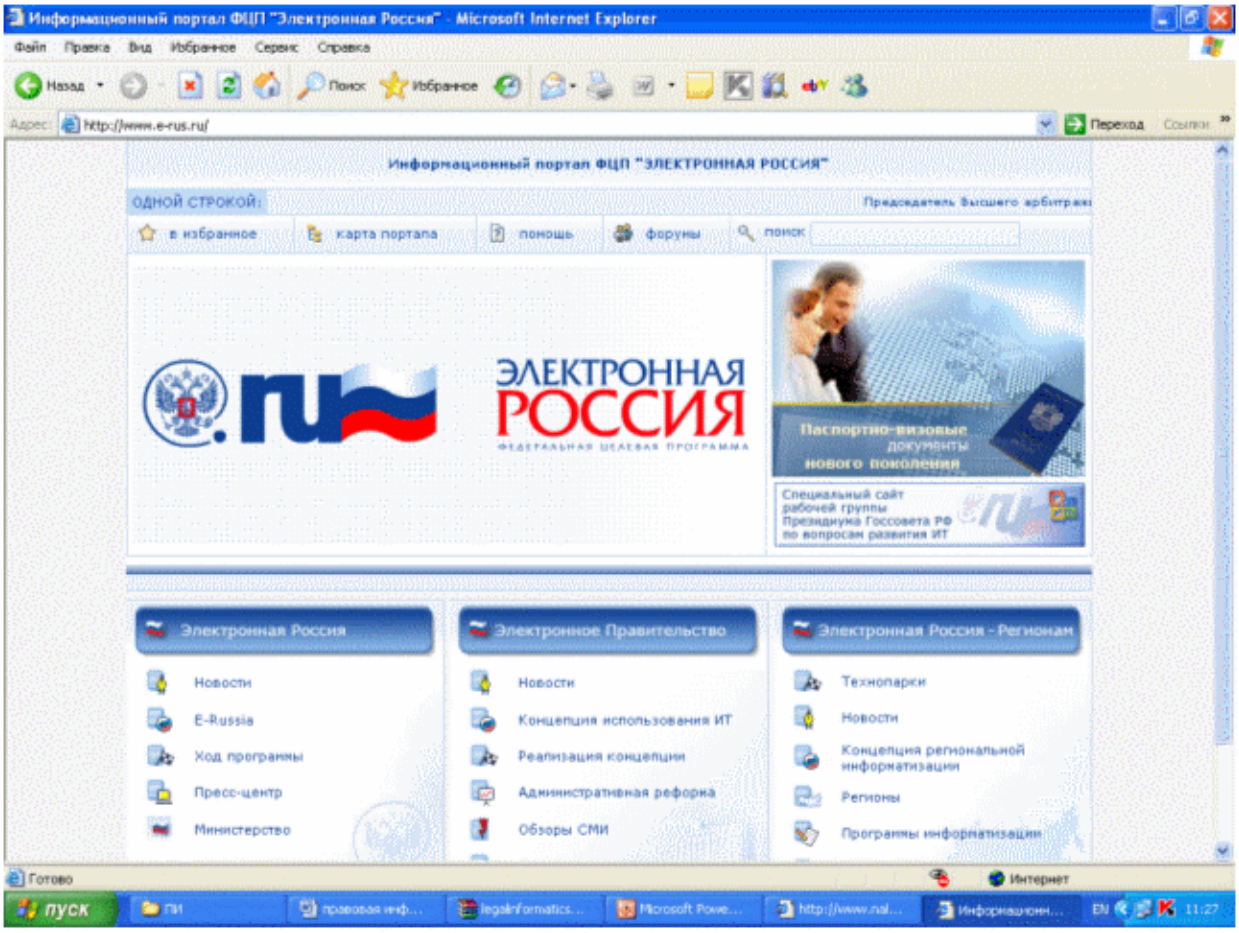
Информация о законопроектах (рис. 2.3).



Подача налоговой отчетности по Интернет (рис. 2.4).



Перспективы развития электронного государства — ФЦП «Электронная Россия (2002-2010)» (рис. 2.5).


Информационный портал ФЦП "Электронная Россия" - Microsoft Internet Explorer
Файл Правка Вид Избранное Сервис Справка
Назад Поиск Избранное
Адрес: http://www.e-rus.ru/
Переход Ссылки
Информационный портал ФЦП "ЭЛЕКТРОННАЯ РОССИЯ"
ОДНОЙ СТРОКОЙ:
Председатель Высшего арбитраж
в избранное
карта портала
помощь
форумы
поиск
.ru
ЭЛЕКТРОННАЯ РОССИЯ
ФЕДЕРАЛЬНАЯ ЦЕЛЕВАЯ ПРОГРАММА
Паспортно-визовые документы нового поколения
Специальный сайт рабочей группы Президиума Госсовета РФ по вопросам развития ИТ
Электронная Россия
Новости
E-Russia
Ход программы
Пресс-центр
Министерство
Электронное Правительство
Новости
Концепция использования ИТ
Реализация концепции
Административная реформа
Обзоры СМИ
Электронная Россия - Регионам
Технопарки
Новости
Концепция региональной информатизации
Регионы
Программы информатизации
Готово
Интернет
пуск
ГИ
правовая инф...
legalinformatics...
Microsoft Powe...
http://www.nal...
Информационн...
EN
11:27

3. Информационно-телекоммуникационные технологии экспертной деятельности и экспертные правовые системы

Использование компьютеров существенно ускоряет экспертную деятельность и уменьшает вероятность ошибок. Основным направлением здесь считается создание автоматизированного рабочего места эксперта по различным видам правоохранительной деятельности, автоматизированных банков данных экспертной информации (автоматизированных информационных систем) и соответствующих программных комплексов для экспертных задач. Можно выделить несколько типичных автоматизированных информационных систем (АИС) и банков криминальных данных.

Пулегильзотеки — для идентификации оружия по пулям и гильзам. Таковы, например, АИС «Модель оружия», «Патрон».

Дактилоследотеки (АДИС) — для анализа снятых на дактилокартах отпечатков пальцев с места происшествия. Принадлежность отпечатков конкретным лицам устанавливается экспертом. Отметим, что отпечатки пальцев с трудом поддаются компьютерному анализу из-за отсутствия устойчивости признаков. Зарубежные дактилоскопические системы имеют высокую стоимость и очень требовательны к качеству отпечатков. Так в ходе недавно проведенного в США снятия отпечатков пальцев у всего населения процедуру снятия у многих лиц приходилось проводить неоднократно для получения качества, приемлемого для компьютерной обработки. Из отечественных дактилоскопических систем наиболее известны «Папилон» и «Сонда-Фрес», которые сейчас активно внедряются в ОВД РФ. Хотя в некоторых странах отпечатки снимаются у всего населения, в РФ — только у лиц, привлекавшихся по уголовным делам. Зачастую, правда, отпечатки снимаются и у лиц «криминогенных категорий», хотя это и противозаконно. Более правильно, конечно, дактилоскопировать все население, поскольку это позволяет опознавать не только преступников, но и потерпевших, в том числе трупы. Сейчас в РФ основная масса дактилокарт составлена на лиц в следственных изоляторах, подследственных или ранее судимых. Но качество

дактилокарт очень низкое, они плохо выполнены, на плохой бумаге и в подавляющем большинстве непригодны для ввода в АДИС. В целом, дактилоскопический учет поставлен пока неудовлетворительно. В правовом отношении не разработаны формальные основания для постановки на дактилоскопический учет. Не снимаются дактилокарты у трупов, слабо используются АДИС, так что множество уже имеющихся дактилокарт почти не используется в следственной практике.

Оптимальная организация единой АДИС (в масштабах региона) должна иметь два уровня:

первый уровень составляют центральный сервер и связанные с ним рабочие станции, часть из которых размещается в городских ОВД. Базы данных в виде дактилокарт и следов с мест преступления хранятся и обрабатываются на центральной станции, имеющей для этого соответствующее программное и техническое обеспечение для их обработки. Ввиду большого объема передачу графической информации с мест на центральный сервер лучше выполнять не с помощью модемной связи, а с помощью DVD дисков или флешек.

второй уровень составляют местные АДИС в удаленных от регионального центра городских ОВД, связанные с центральной региональной АДИС по обмену информацией из баз данных и проведению поиска по запросам.

Такая двухуровневая система оказывается более эффективной и пригодной для организации круглосуточной оперативной работы.

Следотеки — для исследования следов обуви. Эта важная экспертиза пока в РФ развита недостаточно, хотя имеются некоторые системы для анализа следов, например, «Обувь» и «Сапог». Для анализа используется кодирование элементов подошв обуви и рельефа рисунка.

Анализ шрифтов машинописных текстов, в основном ориентированный на шрифты пишущих машинок различного производства. Поскольку сейчас большинство текстов готовится с помощью компьютерных принтеров, этот анализ сильно усложняется, и надо, по существу, заново проводить всю работу по накоплению баз данных с образцами шрифтов.

Имеется также ряд других баз данных и автоматизированных информационных систем криминалистического профиля:

для анализа взрывчатых веществ (АИС «Взрывчатые вещества»);

для анализа текстильных волокон (АИС «Волокно»);

для анализа рентгенограмм (АИС «Фазан»);

для анализа автоэмалей (АИС «Марка»);

для анализа красителей шариковых ручек (АИС «Спектр»);

для анализа стекол автомобильных фар (АИС «Стекло»);

для анализа бумаги (АИС «Бумага»);

для библиотек инфракрасных спектров (АИС «БИРСИ», Германия);

для анализа металлов и сплавов (или их следов).

Создание подобных АИС и баз данных активно продолжается.

Еще одно фундаментальное направление в информационной технологии экспертной деятельности — разработка автоматизированных программных комплексов (АПК) для решения экспертных задач. Примерами могут служить:

АПК «Контакт» для обнаружения контактов волокнистых материалов (например, волокон на одежде);

АПК «Внешняя баллистика» для установления возможности поражения пулей или дробью из огнестрельного оружия;

АПК «ГАЗХРОМ» для криминалистической экспертизы материалов, веществ и изделий из них с использованием газовой хроматографии;

АПК для судебной экспертизы почерков, в том числе умышленно измененных;

АПК для анализа подписей и обнаружения поддельных подписей.

Важную роль в работе эксперта-криминалиста играет автоматизация физико-химических исследований для накопления, хранения, анализа спектров в широком диапазоне частот — от инфракрасного до ультрафиолетового — с использованием обширных библиотек спектров. Здесь применяются также методы электронного парамагнитного резонанса и масс-спектроскопии. Наконец, новые информационные технологии успешно применяются для автоматизации

судебно-фоноскопических экспертиз. Типичные задачи, которые здесь решаются:

идентификация личности по речевому сигналу;

обнаружение монтажа фонограмм;

идентификация звукопроизводящих объектов;

удаление звуковых помех и шумов при распознавании звуков (речи);

распознавание содержания речи по сильно искаженной фонограмме;

распознавание копий и оригиналов фонограмм.

Работы в этой области сейчас активно продолжаются.

Для автоматизации работы эксперта-криминалиста создаются и используются экспертные правовые системы. Экспертные правовые системы (табл. 3.1), как и экспертные системы любого назначения — это системы искусственного интеллекта, включающие базу знаний, правила вывода и механизм вывода («машина вывода»). Экспертные правовые системы позволяют распознавать криминальную ситуацию, находить возможные направления ее расследования, давать практические рекомендации.

Таблица 3.1.

Типовой состав экспертной правовой системы

Правовая экспертная система			
Правила вывода	*Знания*		*Механизм вывода*
Факты	Убеждения	Правила	Базы знаний
Объекты	Атрибуты	Условия	Ограничения

Используемые в экспертной правовой системе знания складываются из фактов, убеждений и правил, а базу знаний составляет информация о предмете расследования в данный момент, которая создается на основе исследований в данной конкретной области и опыта специалистов. База содержит набор правил и факты в виде объектов, атрибутов и условий. Учитываются также ограничения на достоверность фактов. База знаний формируется специалистами в соответствующей области и при функционировании может активно использовать базы

данных. Чтобы ускорить и упростить создание баз знаний, существуют экспертные оболочки, например, «Интерэксперт», Insight, Guru.

В правоохранительной деятельности экспертные системы используются, в основном, в следственной практике, хотя имеются примеры и других применений. Так экспертная система «Блок», предназначенная для борьбы с экономическими преступлениями, позволяет расследовать хищения в строительстве с использованием экономических, технологических, товароведческих, бухгалтерских, оперативных материалов и признаков, а также данных о лицах и документах в этой области. Экспертная система «Блок» может адаптироваться в процессе эксплуатации. Экспертная система «Автоэкс» предназначена для экспертизы дорожно-транспортных происшествий и позволяет, например, установить, мог ли водитель транспортного средства предотвратить происшествие.

Новым классом автоматизированных информационных систем являются системы поддержки принятия решений, которые представляют собой объединение АИС и экспертной системы. К экспертным системам можно также отнести автоматизированные информационно-распознающие системы — сложные системы со специальными техническими и программными средствами.

Для автоматизации судебно-экспертных исследований требуется использование экспертных систем и систем искусственного интеллекта. В этой области можно выделить следующие разделы.

Автоматизация сбора и обработки экспериментальных данных, полученных при расследовании, с использованием современных научно-технических способов. Для этого могут использоваться измерительно-вычислительные комплексы на базе измерительных приборов и компьютеров. Для анализа данных используются технологические банки данных.

Создание банков данных и АИПС по конкретным объектам экспертизы, например, «Металлы», «Автоэмали», «Волокно» (текстиль), «Красители» (волокна), «Помада» (губная), «Бумага», «Оружие», «Наркотические средства». Эти АИПС могут работать самостоятельно или

совместно с другими информационно-вычислительными комплексами. Так, например, имеются АИПС по взрывчатым веществам гражданского и военного применения, а также боеприпасам (можно определять состав, марку взрывчатых веществ по экспериментальным данным); банки данных «Модель оружия-гильзы» (можно найти тип оружия по пуле или гильзе).

Системы анализа изображений, к которым относятся почерки, подписи, отпечатки пальцев, следы обуви, следы от пуль, портреты. Самые трудные проблемы здесь — это фотороботы для реконструкции лица, реконструкция лица по черепу. Некоторые успехи достигнуты с помощью графического процессора Adobe Photoshop.

Вспомогательные расчеты и модели — моделирование криминальных ситуаций (пожаров, взрывов, аварий, дорожно-транспортных происшествий) в зависимости от условий (где возникают, как развиваются). Для различных версий иногда полезно использовать мультипликацию, это помогает составить план расследования. С помощью расчетов можно отличать самодельное оружие от боевого и т.д.

Автоматизированное решение экспертных задач вплоть до подготовки экспертного заключения. Этой цели служат системы поддержки судебной экспертизы (СПСЭ). С их помощью можно провести исследование и оценку вещественных доказательств, подготовить и сформулировать экспертное заключение. Примерами могут служить СПСЭ:

«ЭВРИКА» (экспертиза и выдача результатов исследования кабелей), работающая в диалоговом режиме;

«Кортик» — экспертиза холодного оружия;

«Балэкс» — баллистическая экспертиза;

«Наркоэкс» — экспертиза наркотических веществ

и многие другие. Принцип работы всех СПСЭ — эксперт отвечает на вопросы компьютера. В случае неоднозначности рекомендаций СПСЭ решение принимает эксперт по своим убеждениям. Поскольку СПСЭ может быть очень много, имеются программные средства их автоматизированной разработки для конкретных приложений. Для

работы с СПСЭ желательно использовать «компьютеризованное рабочее место эксперта» с необходимым программным обеспечением. Но эксперт должен понимать математический аппарат принятия решений или работать совместно с математиком.

Создание обучающих систем (тренажеров) с соответствующим техническим и программным обеспечением. Имеются, например, тренажеры «Убийство», «Следователь» и др. Многие СПСЭ имеют тренажеры для овладения методами экспертизы.

Наибольшие успехи пока достигнуты в области сбора и обработки экспериментальных данных; используются СУБД Clipper, Paradox, FoxPro и др. Но организационно и практически многие вопросы еще не решены. Из-за появления новых компьютеров и языков программирования одни и те же программы приходится многократно переделывать. Имеются сложности с применением математических методов в экспертизе и статистических оценках. Часто используемые в расследовании методы индукции могут быть не применимы к случайным событиям, и полученные на их основе выводы могут оспариваться в суде. Многие оценки субъективны, поскольку факторов (причин) очень много и их трудно формализовать. Полная автоматизация здесь вообще вряд ли возможна, и нужны гибридные системы «эксперт + компьютер», т.е. интерактивные СПСЭ, основанные на диалоге эксперта с компьютером, имеющим «дружественный интерфейс».

В сфере ответственности за свои действия следует отметить Федеральный закон от 10 января 2002г. № 1-ФЗ «Об электронной цифровой подписи», целью которого является обеспечение правовых условий использования электронной цифровой подписи в электронных документах, при соблюдении которых электронная цифровая подпись в электронном документе признается равнозначной собственноручной подписи в документе на бумажном носителе. Действие данного Федерального закона распространяется на отношения, возникающие при совершении гражданско-правовых сделок и в других предусмотренных законодательством Российской Федерации случаях.

Применение электронной цифровой подписи предусматривает также проект Федерального закона «О Государственной автоматизированной системе «Выборы». В соответствии со ст. 160 ГК РФ при совершении сделок может быть использована наряду с другими средствами электронная цифровая подпись в случае и в порядке, предусмотренном законом.

В сфере авторского права также не прекращается нормотворчество. Госдума должна была на пленарном заседании 17.09.08г. рассмотреть во втором чтении поправки к закону «О библиотечном деле». Однако в последний момент представители думского комитета по культуре, готовившего поправки, попросили снять законопроект с повестки дня. После того, как против поправок резко выступили известные писатели и издатели, в комитете по культуре решили, что по поводу законопроекта «необходимо дополнительно проконсультироваться с другим комитетом Госдумы — по гражданскому, уголовному, арбитражному и процессуальному законодательству».

Напомним, что поправки к закону «О библиотечном деле» инициированы группой депутатов от «Единой России», в том числе первым вице-спикером Олегом Морозовым. Они были приняты в первом чтении 2 июля 2008 г. Законопроект предлагает «в целях сохранности фондов» наделить правом оцифровывать «любые документы», например, книги, без согласия авторов и без выплаты им вознаграждения три главные библиотеки страны — создаваемую Президентскую библиотеку имени Б.Н. Ельцина, Российскую государственную библиотеку и Российскую национальную библиотеку в Санкт-Петербурге.

Поправки раскритиковали и писатели, и издатели, посчитавшие, что они подорвут книгоиздательский рынок, оборот которого оценивается в $2 млрд. Группа известных писателей, среди которых Сергей Лукьяненко, Людмила Улицкая, Борис Васильев, Полина Дашкова и Борис Стругацкий, обратилась с письмом к президенту Дмитрию Медведеву, заявив, что Госдума предлагает фактическую национализацию авторских прав на любые книги. Они также добавили,

что поправки нанесут им экономический ущерб, так как основные доходы от написанных произведений авторы получают на третий и последующие годы.

Создание электронных копий авторских произведений без согласия авторов противоречит четвертой части Гражданского кодекса РФ, которая гласит, что «исключительное право на произведение» принадлежит автору. Незаконное распространение электронных копий произведений подпадает под действие статьи 146 УК РФ «Нарушение авторских и смежных прав», которая предусматривает до шести лет лишения свободы.

Недовольство литераторов привело к тому, что 11 сентября 2008г. комитет Госдумы по культуре провел расширенное заседание, куда были приглашены писатели, издатели и представители библиотек. Один из идеологов законопроекта полпред правительства в Госдуме Андрей Логинов заверял, что библиотекари не решатся на пиратское распространение оцифрованных книг «под страхом тюрьмы». Оппоненты законопроекта настаивали на том, чтобы право оцифровывать книги получила только библиотека имени Ельцина. При этом она могла бы производить копии книг только при условии выплат авторских отчислений, а средства на это выделялись бы из бюджета. Библиотекари же настаивали на том, чтобы право делать электронные копии книг получили все библиотеки.

«В документе осталось много расширительных толкований. Например, он предполагает использование копий только в стенах библиотек, однако все ведущие библиотеки давно вышли в Интернет, и книги оттуда можно читать в любом удобном месте,— заявил финансовый директор издательства АСТ Олег Бартеньев. — Мы не знаем, в каком виде законопроект будет вынесен на следующее заседание, и можем только надеяться, что авторы законопроекта учтут сделанные замечания». Господин Логинов заявил, что следующая попытка рассмотреть документ в Госдуме будет предпринята 1 октября. «Дополнительные консультации нужны, чтобы снять все разногласия с писательским сообществом»,— объяснил он.

4. Справочные правовые системы

В настоящее время в России интенсивно формируется рынок информационных услуг и технологий. В число инструментальных технологий рыночной экономики активно внедряются компьютерные системы: коммерческие базы данных тематического характера; системы электронных бирж и рекламных досок (объявлений); системы удаленной обработки информации, средства предоставления информационных услуг. Рынок информационных ресурсов опосредует связь между индустрией информации и потребителями информации.

Информационными продуктами являются компьютерные технологии, информационные ресурсы и информационные услуги. Информационная услуга — получение и предоставление в распоряжение пользователя информационных продуктов. Среди данных услуг большое значение играют справочно-правовые системы — это новое поколение справочников, справочники эпохи информационных технологий.

Справочные правовые системы (СПС) — необходимое средство в правоохранительной деятельности при работе с правовой информацией. СПС позволяют:

1) работать с большими объемами информации, которые могут постоянно пополняться;

2) использовать архивы правовых документов;

3) использовать поисковые средства в режиме реального времени;

4) использовать различные средства телекоммуникаций, включая электронную почту, Интернет, компьютерные сети.

Сейчас имеется много СПС, хотя широкое распространение получили всего несколько. Основными характеристиками СПС можно считать:

1) объем информационных ресурсов;

2) метод формирования пользовательской базы;

3) скорость поиска информации (документов, фактов, указаний);

4) актуальность информации;

5) оперативность поступления новой информации;

6) аутентичность документов оригиналу;

7) возможности юридической обработки документов;

8) возможности удаленного доступа к СПС;

9) возможности использования гипертекста. (Под гипертекстом будем, как обычно, понимать «многослойный текст» с переходом к другим информационным блокам с помощью выделенных в тексте «гиперссылок»).

Поиск в СПС осуществляется по названию органа, принявшего документ (решение, приказ, постановление); по названию документа, по дате принятия, по типу документа. После нахождения документ посылается на печать или в файл на компьютере пользователя.

Наиболее используемой в Российской Федерации справочной правовой системой является «Консультант-Плюс», обеспечивающая полное и оперативное включение, обновление, коррекцию всех правовых документов Правительства, Государственной Думы, Центрального Банка и многих других органов. Если какой-либо документ отсутствует в информационной базе СПС, его можно заказать и получить в виде ксерокса или файла. Информационно-поисковая система СПС написана на языке С++, использует мощные поисковые средства, оригинальный формат базы данных и способы индексации. Поиск правовых документов осуществляется по следующим данным:

1) вид документа;

2) регистрационный номер документа;

3) наименование органа, принявшего документ;

4) название документа;

5) ключевые слова. (Под ключевыми словами понимаются несколько, обычно не более 20, слов и словосочетаний, по которым можно понять, чему посвящен документ);

6) название рубрики документа;

7) дата принятия документа;

8) дата и номер регистрации документа в Министерстве юстиции и регистрационный номер;

9) статус документа;

10) слова и словосочетания из текста документа.

Использование в поисковом запросе логических условий дает возможность работать только с новейшими редакциями документов; отбирать лишь документы, полученные при очередном пополнении; отбирать документы, поступившие за некоторый промежуток времени. Заказанную информацию можно получить через сеть Интернет или по телефону. Принятые алгоритмы и форматы обмена данными между Центральным Эталонным Информационным Банком и абонентами сети «Консультант-Плюс» полностью обеспечивают целостность данных, т.е. передачу только новых и измененных документов.

Из полученной информации пользователь может создать собственный информационный банк на своем компьютере. Недостающие документы всегда можно дополнительно заказать из СПС.

СПС «Консультант-Плюс» отличается простотой и удобством работы, имеет высокую степень сжатия информации. В ней используются многоуровневый рубрикатор в виде дерева, сложные поисковые запросы по разным признакам, гипертекст с переходом по ссылкам. При этом возможны два типа ссылок: прямые ссылки, на которые ссылается просматриваемый документ, и обратные ссылки, которые ссылаются на просматриваемый документ. При запросах пользователю передаются только новые и измененные документы.

Пользователь СПС может создавать собственные «папки документов» по различным темам, производить объединение и пересечение множеств документов. Возможна организация коллективной работы нескольких пользователей над одной проблемой. Можно использовать фрагменты документов из Информационного банка СПС, сохранять историю запросов, выполнять многие другие действия, часто встречающиеся в юридической практике.

СПС «Консультант-Плюс» представляет собой объединение нескольких справочных систем — так называемых «версий».

«Арбитраж» — собрание документов Высшего Арбитражного Суда Российской Федерации, Верховного Суда Российской Федерации, обзоры дел в судах, обзоры адвокатской и арбитражной практики.

«Бухгалтер» — нормативные акты, регламентирующие бухучет и налогообложение; консультации квалифицированных специалистов по наиболее часто встречающимся в бухгалтерской практике вопросам бухучета и налогообложения. Имеются две независимые базы данных:

нормативные документы, регламентирующие бухучет и налогообложение;

«Вопросы—ответы» — ответы квалифицированных специалистов на вопросы, часто встречающиеся в бухгалтерской практике.

«Деловые бумаги» — формы деловых документов.

«МоскваПроф» — тексты нормативных актов московской мэрии, Правительства Москвы, Московской Городской Думы, Москомимущества и других московских органов.

«Проф» — справочная система по российскому законодательству, содержащая законы и подзаконные акты, принятые на федеральном уровне.

«Региональные выпуски» — документы местных законодательных органов в свыше 50 регионах Российской Федерации.

«Региональное законодательство» — нормативные акты более чем 58 регионов РФ.

«Россия-СНГ» — многосторонние документы СНГ, двусторонние договора РФ с другими субъектами СНГ.

«Судебная практика» — включает как официальную информацию (документы Высшего Арбитражного Суда РФ, Конституционного Суда РФ, Совета Судей РФ), так и неофициальную информацию (статьи и обзоры о рассмотренных судами делах, образцы исковых заявлений и т.п.). Кроме того, банк данных содержит тексты судебных актов (или извлечения из них) судов разных инстанций. Имеются возможности удобной работы для поиска частей документов, отбора нужных частей, формирования списков документов.

«Финансист» — консультации специалистов (сотрудников государственных ведомств, экспертов ведущих аудиторских и консалтинговых фирм) по вопросам законодательства о финансах и кредитах. Консультации касаются налогов, взносов, платежей, расходов

предприятий, выплат физическим лицам. Имеются словари финансовых и бухгалтерских терминов. Из текста консультации можно переходить в текст нормативного документа, на основании которого дана консультация.

«Эксперт-Приложение» — справочная система, содержащая законы и нормативные акты Российской Федерации, а также документы свыше 80 министерств и ведомств, включая и все документы из версии «Проф».

Справочные правовые системы семейства «Консультант-Плюс» могут распространяться на компакт-дисках, функционируют для аккредитованных пользователей на IBM-совместимых компьютерах, в операционных системах MS DOS, Windows и в локальных вычислительных сетях, доступны через Интернет. Банк данных СПС уже сейчас содержит свыше 2 миллионов документов и практически ежедневно пополняется. В базах правовых данных СПС «Консультант-Плюс» имеется также более 100 тысяч правовых документов многих российских регионов. Пользователи СПС могут вести собственные базы данных.

Популярна также СПС «Гарант» (см. гл. 9), в которой используется гипертекстовая технология хранения правовой информации с еженедельным обновлением информационных ресурсов. Система может работать в операционных системах MS DOS, Windows, OS/2. Информационные ресурсы СПС состоят из 17 банков данных, в которых хранятся правовые документы с 1924г. Имеются также банк данных на английском языке, шестиязычный словарь «Бизнес и право», Информационный банк «Законодательство субъектов РФ».

Еще одной справочной правовой системой является система «Кодекс», имеющая 33 правовых базы данных. СПС «Кодекс» может выполнять много операций, например, формировать «Перечень документов по тематике», «Выборку документов по признакам». При этом можно задавать «Условия выборки», меняя и добавляя условия для поиска. Достоинство СПС — активное использование меню и оконной технологии. В верхней части окна «Документы» выдается список документов, а в нижней части — название и атрибуты текущего

документа. По умолчанию документы располагаются по алфавиту, но можно рассортировать их и по дате принятия, виду, номеру. В окне «Текст документа» можно просмотреть и обработать текст документа. Можно находить документы, связанные с данным документом; создавать и вести произвольное число собственных баз данных.

Необходимо отметить, что юридическая информация на магнитных носителях обычно не имеет юридической силы и обязательно требуется ссылка на печатное издание. Отметим, что в США имеются прецеденты использования Википедии (виртуальный словарь, расположенный в Интернете и редактируемый пользователями), как юридической информации для вынесения приговоров в судах. Требуемые ссылки помещаются в базах данных СПС. Информация в базах данных справочных информационных систем может служить только для справок, на нее нельзя ссылаться в суде. Вопрос возмещения материальных убытков из-за неполноты или неточности данных в базах данных СПС законодательно не регламентируется и пока решается разработчиками СПС.

Поэтому СПС пока следует рассматривать лишь как удобное, но не всемогущее вспомогательное средство в юридической деятельности.

Порядок получения правовой информации определяется законодательством о средствах массовой информации. В соответствии с требованиями ст. 23 Конституции РФ не может использоваться информация, содержащая сведения о частной жизни граждан. Юридические учреждения активно участвуют в проводимой органами СМИ работе по освещению фактов и явлений правовой жизни.

Дополнительные возможности открывает Закон РФ «О средствах массовой информации» (с изменениями и дополнениями). Первостепенное значение имеют ст.ст. 38 и 39 Закона. Согласно ст. 38 граждане вправе оперативно получить через СМИ достоверные сведения о деятельности государственных органов и организаций, общественных объединений, их должностных лиц. В соответствии со ст. 39 редакция СМИ имеет право запрашивать (в устной и в письменной форме)

информацию о деятельности государственных органов и организаций, общественных объединений, их должностных лиц.

Федеральный закон от 13 января 1995г. № 7-ФЗ «О порядке освещения деятельности органов государственной власти в государственных средствах массовой информации» регулирует отношения, возникающие в связи с распространением государственными СМИ материалов или сообщений о деятельности органов государственной власти Российской Федерации и ее субъектов.

Вопросы деятельности СМИ в сфере правовой информации регулируются и в подзаконных актах. В частности, в Указе Президента РФ «О дополнительных гарантиях права граждан на информацию» установлено, что деятельность государственных органов, организаций и предприятий, общественных объединений, должностных лиц осуществляется на принципах информационной открытости, что выражается:

в доступности для граждан информации, представляющей общественный интерес или затрагивающей личные интересы граждан;

в систематическом информировании граждан о предполагаемых или принятых решениях;

в осуществлении гражданами контроля за деятельностью государственных органов, организаций и предприятий, общественных объединений, должностных лиц и принимаемыми ими решениями, связанными с соблюдением, охраной и защитой прав и законных интересов граждан;

в создании условий для обеспечения граждан Российской Федерации зарубежными информационными продуктами и оказания им информационных услуг, имеющих зарубежное происхождение.

Из сказанного можно сделать следующий вывод: развитие законодательства за последние годы сформировало нормативную базу деятельности СМИ в правовой сфере. Вместе с тем это законодательство фрагментарно, оно нуждается в упорядочении и приведении в стройную систему.

5. Автоматизированные аналитико-статистические информационные системы, системы учета и управления

Автоматизированные аналитико-статистические информационные системы предназначены для сбора и обработки большого объема первичной информации; результаты обработки представляются в виде таблиц и графиков. Накопленная информация может выдаваться по запросам, т.е. система может выполнять справочные функции. В настоящее время существует несколько аналитико-статистических информационных систем, из которых отметим следующие системы.

1. Справочная информационно-аналитическая система Государственной инспекции по безопасности дорожного движения (ГИБДД).

Система предназначена для сбора, накопления, анализа информации и подготовки отчетов по авариям на транспорте. Основными задачами системы являются ведение и корректировка статистики дорожно-транспортных происшествий (ДТП) по регионам и годам, оценка показателей аварийности, прогнозирование статистики ДТП, сравнительный анализ ДТП по разным регионам, ранжирование регионов по уровню ДТП. Система предназначена для пользователей, плохо владеющих табличными процессорами (например, Excel). С помощью системы можно:

вводить новые статистические показатели;

корректировать введенные показатели;

получать информацию из баз данных;

представлять выборки по годам и регионам в виде таблиц;

формировать отчеты;

прогнозировать аварийность с помощью экстраполяционных моделей;

выявлять регионы с меньшей аварийностью.

2. Автоматизированная информационная система «Кадры».

Система предназначена для управления кадрами и может в интерактивном режиме:

накапливать информацию о кадрах;

анализировать кадровый состав;

рассчитывать выслугу лет (для присвоения очередных званий работникам органов, вычисления пенсий);

автоматически готовить кадровые документы и справки по кадрам;

осуществлять контроль за кадрами;

управлять доступом к данным по кадрам;

выдавать кадровые документы в различной форме;

производить поиск документов по заданным критериям;

выводить на печать кадровые документы в требуемой форме;

готовить статистические данные по кадрам.

3. Автоматизированная информационная система «ГРОВД».

Система «ГРОВД», разработанная Академией МВД, функционирует на базе сети персональных компьютеров и предназначена для информационного обеспечения оперативно-розыскной и управленческой деятельности городских и районных органов внутренних дел. Система помогает решению следующих классов оперативно-розыскных задач:

«лица»;

«преступления»;

«похищенные вещи»;

«оружие»;

«нераскрытые преступления»;

«учет заявлений и преступлений»;

«статистика»;

«автомототранспорт».

Работа системы строится на основе первичных документов (карточек). Функциями системы являются:

защита информации от несанкционированного доступа с помощью паролей и других средств;

накопление, коррекция и поиск сведений по указанным выше классам задач;

вывод сведений в требуемой форме;

сортировка записей по заданным критериям (по алфавиту, по датам и т.п.);

уточнение запросов на выдачу данных в ходе поиска;

проверка других массивов данных на наличие записей, релевантных запросу (например, связь лица с преступлением, оружием, транспортными средствами);

изменение первичных документов без потери информации.

АИС «ГРОВД» — открытая система и поэтому допускает пополнение средствами решения новых задач. Имеется несколько версий этой довольно широко используемой АИС.

4. АИС сбора и обработки данных «Охрана».

АИС «Охрана» предназначена для службы охраны МВД и позволяет вводить, хранить, корректировать сведения:

об объектах охраны;

о средствах охраны;

о численности охраны;

о лицах, причастных к хищениям;

о работе и дисциплине персонала охраны.

Можно также вводить и корректировать сведения из подразделений службы охраны МВД о кражах, хищениях, объектах охраны, ложных тревогах. По всем имеющимся в системе данным можно готовить и выдавать статистические отчеты за год, квартал, месяц; отчеты по отдельным подразделениям МВД и др.

5. Справочная информационно-аналитическая система ГУ Охраны РФ.

Система предназначена для руководящего персонала, мало знакомого с табличными процессорами, и служит для сбора, накопления, анализа, подготовки отчетов по основным показателям службы охраны. Основные задачи системы — накопление, статистическая оценка, корректировка важнейших показателей службы охраны в регионах по годам; получение и прогнозирование абсолютных и относительных статистических оценок деятельности службы. Система позволяет в диалоговом режиме:

вводить новые статистические показатели;

корректировать старые показатели;

определять состояние базы данных по регионам и годам по разным показателям;

получать выборки абсолютных и относительных показателей по годам и регионам в виде готовых для отчетов таблиц;

улучшать таблицы (например, сортировать строки-регионы);

осуществлять прогнозирование путем экстраполирования;

выводить найденный прогноз в виде таблиц или диаграмм.

6. Автоматизированная система управления «РОВД».

АСУ «РОВД» предназначена для информационно-аналитических подразделений районных отделений органов внутренних дел. Информационно-поисковая система «Слежение», представляющая собой подсистему АСУ «РОВД», служит для ввода, хранения, корректировки, выдачи данных для информационно-аналитических отделов РОВД. В ИПС «Слежение» имеются следующие виды учета:

«КУП» — заявления и сообщения о преступлениях и происшествиях, сведения об их расследовании, об уголовных делах для поиска похищенного, об оперативной работе (задержанные лица), об угнанном транспорте;

«Форма 1» — статистическая карточка на преступление, составленная на основе «КУП»;

«Форма 1.1» — статистическая карточка о результатах расследования, раскрытии преступления, деятельности следователей;

«Форма 2» — статистическая карточка на преступника;

«Форма 3» — статистическая карточка о прохождении дела и решении;

«Форма 6» — статистическая карточка о результатах суда.

В АСУ «РОВД» имеется ряд программ для ввода информации о событиях, лицах, объектах, представляющих оперативный интерес; для хранения и корректировки данных, для управления данными; для выявления связей между различными видами информации по конкретному событию, лицу, объекту; для ввода, хранения,

корректировки кодов предметов, преступников, происшествия, места происшествия, способа совершения преступления; для интерактивных запросов, для подготовки необходимой отчетности.

7. Автоматизированная система паспортного отделения («АСПО»).

Система АСПО предназначена для автоматизации работы паспортных столов в районных отделениях внутренних дел и содержит информацию о данных на конкретное лицо и на его родственников; о паспортах, прописке и выписке; об утраченных и похищенных паспортах, о судимости некоторых категорий лиц (должники, неплательщики алиментов), о паспортных правонарушениях, об административном надзоре за лицами, о выездах за рубеж. По запросам на экран дисплея может выдаваться полное досье на лицо; досье может пополняться. Система обеспечивает достаточно гибкую работу, даже с переводом на другие языки. Возможно ограничение доступа с использованием паролей, кодов и других средств. Для сохранения информации можно автоматически создавать ее дубли. Обычно «АСПО» входит в локальную вычислительную сеть районного ОВД.

На основе АСПО легко вести учет избирателей. Центризбирком РФ 9 сентября 2008г. объявил о проведении эксперимента по голосованию через Интернет. Он состоялся 12 октября на выборах депутатов муниципального собрания Новомосковска Тульской области. С технической точки зрения эксперимент удался, и это может открыть дорогу для внесения в избирательное законодательство поправок, разрешающих голосование через Интернет.

Действующее законодательство не разрешает голосование через Интернет, поэтому эксперимент, который проводил ЦИК, считается электронным опросом избирателей. Для наблюдения за ходом эксперимента были приглашены наблюдатели от партий, впрочем, по словам главы ЦИКа Владимира Чурова, они дали подписку о неразглашении технических подробностей. Кроме того, господин Чуров сообщил, что в ходе встречи с новым директором Бюро по демократическим институтам и правам человека (БДИПЧ) ОБСЕ Янешем

Ленарчичем была достигнута договоренность о присутствии в Новомосковске представителей БДИПЧ.

Эксперимент охватил пять участков. В нем приняли участие около 10% от числа проголосовавших и это считается хорошим результатом. В абсолютных цифрах участниками эксперимента стали минимум 500 человек. На эксперимент потратили 1 млн. руб. его готовили Федеральный центр информатизации при ЦИКе совместно с ФГУП «Восход», разрабатывавшим ГАС «Выборы».

Избирателям на выходе с обычных избирательных участков предлагали продублировать свое волеизъявление при помощи диска для электронного голосования. Активировать диск можно было на компьютере в специально оборудованном здесь же Интернет-киоске или на любом, в том числе домашнем, компьютере. Согласно описанию технологии экспериментального опроса, предоставленному в ЦИКе, диск дает право однократного доступа в часы голосования к специальному серверу, на котором избирателю открывается электронный опросный лист. Доступ к серверу и информация на нем о том, кому отдал свой голос конкретный избиратель, были даны оператору «со специального автоматизированного рабочего места — комплекса программно-технических средств» после окончания голосования. Сопоставляли результаты электронного опроса с итогами специального соцопроса, который ЦИК проводил до и после дня голосования (не с данными самого голосования).

Как уже говорилось эксперимент удался с технической точки зрения, в дальнейшем он может быть применен в труднодоступных местах для голосования — на судах дальнего плавания, в труднодоступных районах Крайнего Севера и т.д. Для этого, правда, придется внести изменения в федеральное законодательство. Член думского комитета по информационной политике, информационным технологиям и связи справоросс Илья Пономарев является сторонником голосования через Интернет, поскольку, с его точки зрения, он ничем не отличается от подсчета голосов через применяемую сейчас систему ГАС «Выборы». При этом он признает, что такой способ голосования уязвим.

«Все равно обеспечить анонимность голосования через Интернет с домашнего компьютера невозможно. Надо идти дальше — ввести персональный чип для каждого избирателя по принципу биометрических паспортов — пусть им голосует всегда», — считает господин Пономарев. С его точки зрения, доверие к организаторам выборов обеспечить можно, лишь открыв общественности доступ к так называемым исходным кодам, чертежам операционной системы. Успешные примеры функционирования открытых операционных систем есть. Однако разработчики всех избирательных технических средств ФГУП «Восход» придерживаются обратного принципа, максимально сокращая доступ к информации. Глава Федерального центра информатизации Михаил Попов лишь обещает, что «безопасность будет обеспечена».

Глава общественного объединения «Голос» Лилия Шибанова заявляла, что ЦИК планировал пригласить к обсуждению эксперимента группу экспертов, однако этого не произошло. Она считает, что эксперимент в обнародованном виде опасен для страны, где доверие к выборам весьма невысоко. «Я не сомневаюсь, что изменить законодательство будет очень просто, но голосование через Интернет станет способом для различных злоупотреблений», — считает госпожа Шибанова. Технологии негативного использования принятой схемы, например, появление кандидатов, скупающих диски для голосования, уже обсуждают и в кулуарах ЦИКа.

6. Информационные технологии следственной и оперативно-розыскной деятельности

Новые информационные технологии могут успешно использоваться в следственной деятельности. С их помощью рекомендуется решать следующие основные задачи:

автоматизация следственной работы при создании документов;

автоматизация составления календарных планов и графиков расследования;

сбор, накопление и анализ информации по следственным делам (особенно со многими лицами и эпизодами), автоматизация составления по результатам анализа следственных документов и заключений;

получение справочной информации по уголовным делам из многих источников;

разработка автоматизированных методов расследования по различным видам преступлений;

статистический анализ расследуемых уголовных дел;

автоматизация контроля хода следствия и соблюдения сроков расследования;

создание, ведение, использование баз данных следственной информации;

анализ информации о прошлых преступлениях.

Автоматизация процесса раскрытия преступлений — наиболее сложная задача правовой информатики, хотя вполне можно автоматизировать составление следственных документов, отнимающее много времени. Существенную помощь может оказать «Специализированная территориально-распределенная автоматизированная система Следственного комитета РФ» («СТРАС-СК») с банками данных, включающая три уровня:

1) для центрального аппарата Следственного комитета;

2) для следственных управлений (отделов) МВД-УВД;

3) для следственных подразделений городских и районных органов внутренних дел.

Информационное обеспечение СТРАС-СК состоит из ряда подсистем по следующим направлениям.

«Расследование». По данным о составе, способе, месте, объекте, жертве преступления компьютер выдает рекомендации для планирования расследования, автоматизирует составление документов, поиск и сопоставление материалов по другим делам.

«Контроль». Автоматизируются контроль деятельности следователя (дело «на контроле»), ведение каталога дел, планирование и соблюдение сроков.

«Статистика». Формируются и анализируются статистические данные, ведется накопление данных о преступлениях, лицах, ущербе. Автоматизируются составление обзорных и статистических отчетов, анализ работы конкретного следователя, выдача различных видов статистической информации.

«Справочные системы» по законодательству, нормативным актам и постановлениям, касающимся работы следователя.

«Банки данных» по различным категориям уголовных дел.

«Подсистема связи с банками криминальной информации» (Федеральным и региональными) для получения информации из учетов.

Подсистемы для автоматизации работы секретариата, канцелярии, учета кадров следственного аппарата.

Но в целом система СТРАС-СК еще находится в процессе дальнейшей разработки.

Реализация компьютерных технологий в деятельности следователя может осуществляться с использованием автоматизированного рабочего места следователя (АРМС). Такие рабочие места создаются на базе персональных компьютеров локальной или глобальной сети МВД и снабжаются соответствующим программным обеспечением.

Программное обеспечение процесса расследования уголовного дела дает возможность выполнять такие трудоемкие действия, как:

создание следовательских документов (протоколов, постановлений, запросов, карточек и т.п.);

получение информации (справок) по запросам;

анализ документов (обвинительного заключения, обвинения, постановления о прекращении уголовного дела и др.);

заполнение документов, в том числе различных бланков;

отыскание необходимых сведений в материалах дела (фамилии, имена, отчества; клички, даты, эпизоды, протоколы, места происшествий и др.);

оформление материалов;

составление планов профилактических мероприятий;

систематизация материалов дела;

составление формулы обвинения;

составление обвинительного заключения и других документов по делу;

подготовка материалов для суда.

Для ускорения работы могут использоваться стандартные (типовые) бланки и образцы документов.

Программное обеспечение для обработки сопутствующей информации обеспечивает:

получение информации о фигурантах по уголовному делу;

поиск и анализ связей фигурантов;

получение сведений о вещественных доказательствах;

поиск и анализ данных об эпизодах преступления (место, время, участники, способы совершения, вещественные доказательства и др.).

С помощью этого программного обеспечения автоматизируются поиск, анализ и выдача информации о лицах по делу и их связях, о вещественных доказательствах, эпизодах, сходных происшествиях. Основными требованиями к программному обеспечению АРМС должны быть:

эффективная работа с текстовой информацией и документами;

проверка грамматики документов;

печать документов;

ведение архивов стандартных форм документов и отчетов;

поиск и компоновка текстовых фрагментов;

автоматизированный подбор данных для таблиц;

простейшие статистические расчеты;

поиск и анализ информации;

работа в диалоговом режиме.

Для следственной деятельности разработан ряд автоматизированных информационных систем. Одной из таких систем является «Диалоговый конструктор БИНАР-3» для информационного обеспечения принятия решений, информационно-логических задач, анализа связей и объектов в уголовном деле. БИНАР-3 может хранить и обрабатывать структурированные символьные и числовые данные, а также текстовые фрагменты; имеет средства настройки баз данных и получения отчетов по запросам. База данных конструктора состоит из так называемых объектов учета, включающих:

информацию по делу (учетная карточка, эпизоды, лица, организации);

источники документов (показания лиц, описание вещественных доказательств, сведения о документах по делу).

База данных может включать много сведений (до миллиона записей по каждому объекту учета). На экран или на принтер могут выводиться:

реквизиты учитываемых объектов и связанных с ними объектов;

перечень прямых и косвенных связей большой глубины, т.е. с большим числом звеньев в цепочке связей;

статистические данные о лицах, суммах, эпизодах;

сведения о лицах, фигурирующих в базах данных;

материалы допросов;

фрагменты обвинительных заключений;

взаимосвязи эпизодов, лиц, объектов.

Имеется календарный план расследования по дням и часам. Для работы конструктора используется СУБД Clipper; ряд программных модулей составлен на языке Ассемблера и языке С. Диалоговый конструктор удобно использовать в локальной сети с распределенной базой данных для коллективной работы следственной бригады.

Система анализа и учета уголовных дел САУД-М функционирует на основе интегрированного пакета прикладных программ МАСТЕР. В САУД-М входят:

текстовый процессор;

табличный процессор;

простая СУБД;

ППП для графического отображения данных;

пакет для электронной телекоммуникации;

программы систематизации и анализа материалов дела;

программы учета фигурантов;

программы учета и анализа объектов преступных посягательств; времени, места, способа совершения, мотивов преступления.

Работа САУД-М организуется с помощью меню, как в ОС Windows. Имеются готовые бланки документов, удобно анализируются связи между различными следственными данными. Недостаток системы — невозможность работы в локальной вычислительной сети.

Большие возможности открывает гипертекстовая система ИНТЕЛТЕКСТ, предназначенная для создания текстовых документов (отчетов, обзоров, рекомендаций, обоснований, результатов анализа). С ее помощью можно вести базу текстовых документов, устанавливать связи между ними, строить комбинированные тексты, создавать фрагменты текстов из первичных документов и компоновать их. Работа основана на оконной технологии. Для поиска фрагментов используются ключевые слова, рубрики (типы фрагментов: допросы, показания, протоколы, лица и др.), ссылки на источники фрагмента. Для источников составляется каталог. Для каждого фрагмента имеется набор атрибутов в виде меню. По комбинации атрибутов можно находить фрагмент и запоминать его в соответствующих папках, для которых имеется каталог папок. Папки можно просматривать и корректировать. Фрагменты могут иметь двунаправленные смысловые связи с другими фрагментами. Благодаря связям фрагменты могут объединяться в смысловую сеть в виде гипертекста. Связи могут указываться пользователем (например, по ключевым словам) в интерактивном или автоматическом режиме. По

смысловой сети можно осуществлять навигацию автоматически или вручную. Созданная тематическая подборка затем преобразуется в единый текстовый документ, редактируется и отправляется в файл или на принтер. Само текстовое окно может иметь до трех полей: собственно текст, аннотация, заголовок. Допускаются «прокрутка», изменение размеров окна, масштабирование и другие редакционные действия. Информацию в базе текстовых документов можно отыскивать по строке текста, заголовку, строке аннотации и другим признакам.

АРМС для расследования конкретных видов преступлений разрабатываются Следственным комитетом МВД РФ совместно с ВНИИ МВД и предназначены для автоматизации методики раскрытия таких типичных преступлений, как, например:

грабежи и разбойные нападения;

кражи из жилищ;

незаконный оборот наркотиков.

АРМС для расследования грабежей и разбойных нападений имеет обширный банк данных, основанный на эмпирических исследованиях, нормативных актах и специальной литературе. АРМС включает три блока:

уголовно-правовую квалификацию грабежей и разбойных нападений;

методику расследования грабежей и разбойных нападений;

справочный архив.

Методика расследования — это рекомендуемые следственные действия для различных случаев, а именно:

имеются или не имеются подозреваемые;

имеются или не имеются свидетели;

имеются или не имеются потерпевшие;

каковы вид и способ преступления (грабежа, нападения);

применялось ли оружие;

каков вид применявшегося оружия;

применялось ли насилие;

каковы другие характеристики преступления.

Даются рекомендации по осмотру места происшествия, экспертизе оружия, проведению допросов и другим следственным действиям. Указываются рекомендуемые экспертизы по каждой категории преступлений. Приводится словарь жаргонных слов уголовного лексикона.

АРМС по расследованию краж из жилищ также имеет три блока:

уголовно-правовую квалификацию краж;

методику расследования;

типовые версии.

Блок методики расследования предназначен для работы в диалоговом автоматизированном режиме с учетом разнообразных данных о происшествии:

задержаны подозреваемые или нет;

где задержаны;

подозреваемый явился сам или нет;

потерпевший известен или нет;

есть ли свидетели;

каков способ совершения преступления;

как осуществлено проникновение в жилище и т.п.

Даются рекомендации по осмотру и анализу места происшествия, порядку опознания лиц и предметов, проведению допросов, возможным экспертизам. В блоке типовых версий приводятся возможные предположения о личности преступника.

Программное обеспечение АРМС по расследованию незаконного оборота наркотиков содержит следующие блоки:

выдвижение версии;

методику расследования;

обстоятельства, подлежащие выяснению;

словари (жаргонные термины, названия наркотических средств, синонимы их названий, способы употребления, криминалистические рекомендации);

пояснения (классификацию наркотических средств, краткие сведения о них);

формы следственных документов.

Версии выдвигаются в зависимости от исходных данных. Методика расследования зависит от обстоятельств дела, например:

подозреваемый задержан, известен, не известен;

оперативные данные (подозреваемый задержан с поличным или по другим причинам);

есть ли свидетели или очевидцы;

цель действий задержанного (задержанных): сбыт наркотических средств или без сбыта.

АРМС предназначено для работы в интерактивном режиме и не требует специальной подготовки по ее освоению.

Имеется также специальная информационная система (СИС), предназначенная для автоматизации следственных действий, анализа работы следователей и следственных отделов, управления их работой. Система имеет несколько модулей.

Учет уголовных дел (обвиняемые, подозреваемые, потерпевшие, свидетели; дела в целом).

Работа с документами — формирование следственных документов по уголовным делам, вплоть до обвинительного заключения.

Контроль сроков выполнения расследования и оформления документов.

Архив уголовных дел (хранение исполненных документов и дел, направленных в суд).

Модуль отчетности (статистика уголовных дел, статистический учет).

Сервис (справочники и вспомогательная информация).

Настройка (на аппаратные средства, обслуживание баз данных, копирование информации).

Пользователь устанавливает для СИС расчетный период, в течение которого все документы сохраняются в оперативном ведении; по истечении расчетного периода документы отправляются в архив. Существуют локальный и сетевой варианты системы. Локальный вариант предназначен для следственных подразделений с малой нагрузкой (с

одним компьютером), сетевой — для подразделений с большим объемом работы (с несколькими компьютерами и сетевым программным обеспечением).

Отметим, наконец, следственные экспертные системы, применяемые для раскрытия и расследования преступлений.

Экспертная система прогнозирования преступлений, позволяющая оценить зависимость между характерными особенностями личности преступника и возможным местом совершения преступления.

Экспертная система выявления скрытых преступлений (например, скрытых хищений в производстве или торговле) на основе анализа деятельности предприятий позволяет получить материал для ревизий.

Экспертная система поиска и установления личности преступника позволяет сделать предположения о личности преступника по материалам следствия и сузить круг подозреваемых лиц.

Экспертные системы расследования убийств, анализирующие следственные данные о преступнике, потерпевшем, способе совершения и сокрытия преступления, орудии убийства, возможных мотивах, месте и времени преступления. Такие экспертные системы могут иметь несколько разновидностей в зависимости от криминалистической характеристики преступления (убийство на сексуальной почве, с расчленением трупа, с особой жестокостью и др.).

Экспертные системы для расследования грабежей и разбоев и многие другие.

Широкое использование новых информационных технологий в следственной деятельности позволит поднять ее на более высокий уровень, но пока это использование лишь внедряется, учитывая, в частности, появление все новых видов преступлений, таких, например, как терроризм (в том числе — действия террористов-смертников), захват заложников, похищение людей, изготовление и сбыт фальшивой продукции и др. Важнейшей задачей здесь является создание технического и программного обеспечения, необходимого для решения рассмотренных выше разнообразных правовых задач пользователями, не являющимися специалистами в области прикладной информатики, т.е. с

максимально «дружелюбным к пользователю» интерфейсом. Пока эта задача еще очень далека от выполнения.

7. Компьютерные преступления

Под компьютерными преступлениями понимаются предусмотренные законом общественно-опасные деяния с использованием компьютерной техники. С компьютерными преступлениями тесно связана информационная безопасность.

Проблема информационной безопасности возникла достаточно давно и имеет глубокие исторические корни. До сравнительно недавнего времени методы защиты информации были в исключительной компетенции спецслужб, обеспечивающих безопасность страны. Однако новые технологии измерения, передачи, обработки и хранения информации значительно расширили сферы деятельности людей, нуждающихся в защите информации, привели к развитию и распространению новых методов несанкционированного доступа к информации и, как следствие, к интенсивному развитию нового научного направления — «информационная безопасность». Все это связано, прежде всего, с появлением систем обработки данных на базе компьютеров, а также с бурным развитием систем передачи данных.

Можно выделить некоторые причины, которые и привели к необходимости как разработки новых методов защиты информации, так и к дальнейшему развитию традиционных.

Первые системы коллективного пользования ЭВМ, а затем объединение их в глобальные и локальные сети, технологии открытых систем уже на первом этапе выявили потребность в защите информации от случайных ошибок операторов, сбоев в аппаратуре, электропитании и т.п. Стремительный рост емкости внешних запоминающих устройств и высокая эффективность их использования в системах автоматизированного управления привели к созданию банков (баз) данных колоссальной емкости и высокой стоимости, одновременно создавая проблемы их защиты как от разнообразных случайностей, так и от несанкционированного доступа.

Современные информационные системы составляют техническую основу органов управления государственной власти, промышленных

предприятий и научно-исследовательских организаций, учреждений кредитно-финансовой сферы, банков и т.п. Сегодня, когда компьютер прочно вошел в наш быт, мы все чаще вынуждены доверять ему свои секреты (финансовые, промышленные, медицинские и др.), и в связи с этим вопросы защиты информации приобретают всеобъемлющий характер.

Преступления, связанные с компьютерами, можно разделить на две категории (табл. 7.1). В первой категории компьютер и (или) компьютерная информация является объектом преступления. (Компьютерная информация — это информация на машинном носителе или передаваемая по каналам связи в форме, доступной компьютеру). К этой категории относятся хищение или нанесение ущерба техническим средствам и информации, несанкционированный вредоносный доступ к компьютерной системе и информационным ресурсам. Во второй категории компьютер служит орудием преступления. Таковы, например, осуществляемые с помощью компьютера банковские хищения; государственный, коммерческий, промышленный шпионаж; распространение компрометирующей информации, фальсификация результатов голосования и т.п. Обе категории преступлений тесно взаимосвязаны: например, компьютер может служить орудием несанкционированного доступа к другому компьютеру.

Таблица 7.1.

Компьютерные преступления

Компьютер как объект преступления	Компьютер как орудие преступления
Хищение технических средств и компьютерной информации	Банковские хищения
Повреждение технических средств и компьютерной информации	Шпионаж (государственный, промышленный, коммерческий)
Несанкционированный доступ к техническим средствам и информационным ресурсам	Фальсификация результатов голосования
	Распространение компромата

Различают следующие криминологические группы компьютерных преступлений.

Экономические преступления — самые распространенные, осуществляются с корыстными целями (мошенничество; хищение программ, услуг, компьютерного времени; экономический шпионаж).

Преступления против личных прав и частной сферы (сбор компрометирующих данных о лицах; разглашение банковской, врачебной и другой частной информации; получение данных о доходах или расходах).

Преступления против государственных и общественных интересов (ущерб обороноспособности, фальсификация результатов голосования).

К преступному вмешательству в работу компьютера относится:

Несанкционированный доступ к компьютерной информации в корыстных целях. При этом может использоваться чужое имя, изменение физических адресов технических устройств, остаточная информация, модификация информации и программного обеспечения, подключение записывающих устройств к каналам связи, маскировка под законного пользователя путем раскрытия его пароля (если нет средств аутентификации). При наличии незащищенных файлов несанкционированный доступ возможен и вследствие поломки.

Разработка и распространение «компьютерных вирусов», которые могут распространяться и заражать другие компьютеры; «логических или временных бомб», которые срабатывают при определенных условиях или по достижении определенного времени и полностью или частично выводят из строя компьютерную систему, а также «червей».

Халатная небрежность при разработке и эксплуатации программного обеспечения компьютерной системы, которая может привести к тяжелым последствиям. Но полной надежности быть не может, в программах всегда могут остаться незамеченные ошибки.

Подделка и фальсификация компьютерной информации. Например, при выполнении контрактных работ можно таким путем выдать вновь разработанные негодные компьютерные системы и программное обеспечение за годные и сдать заказчику. Можно фальсифицировать результаты выборов, референдумов, опросов. Возможна и фальсификация в корыстных целях.

Хищение программного обеспечения. В РФ значительная часть программного обеспечения распространяется путем краж, продажи краденого, обмена краденым. Таковы, например, известные «пиратские» компакт-диски, которые значительно дешевле лицензионных и поэтому широко применяются пользователями компьютеров. Бороться с этим видом хищений очень трудно.

Несанкционированное копирование, модификация, уничтожение информации. Преступное присваивание информации может осуществляться путем копирования. Информация должна представлять собой самостоятельный объект охраны.

Несанкционированный просмотр или хищение информации из баз данных, банков данных, баз знаний.

В информационном обществе резко увеличивается число компьютерных преступлений и их доля в общем числе преступлений. Потери могут быть огромными. Имелись покушения на компьютерные хищения на $500000, 70 млрд. руб. и многие другие, произошли хищения на несколько десятков миллионов рублей. Очень большие компьютерные хищения происходят из банков по фиктивным документам. Большинство банковских хищений остаются безнаказанными, поскольку банки обычно не заинтересованы в проведении следствия, опасаясь потери репутации и неизбежного раскрытия банковской тайны.

Предупреждение компьютерных преступлений включает технические, организационные и правовые меры.

К техническим мерам относятся:

аппаратная защита от несанкционированного доступа;

резервирование особо важных компонент компьютерной системы;

организация вычислительных сетей с перераспределением ресурсов при нарушении функционирования;

устройства обнаружения и тушения пожаров;

обнаружение утечек воды;

аппаратная защита от хищений, саботажа, диверсий, взрывов;

дублирование электропитания;

надежные запирающие устройства;

средства сигнализации.

К организационным мерам относятся:

охрана помещений;

подбор надежного персонала;

подготовленный план восстановления компьютерной системы после выхода из строя;

обслуживание и контроль работы компьютерного центра персоналом, не заинтересованным в сокрытии преступлений;

организация защиты информации от всех, включая руководство;

ограничение доступа к компьютерной системе;

выбор безопасного местонахождения информационного центра;

меры административной ответственности.

К правовым мерам относятся:

разработка правовых норм ответственности, усовершенствование уголовного и гражданского законодательства, а также судопроизводства по делам, связанным с компьютерными преступлениями (правовые нормы, предусмотренные в настоящее время Уголовным кодексом РФ, указаны далее в разделе 8);

защита авторских прав программистов;

общественный контроль за разработчиками компьютерных систем;

принятие необходимых международных соглашений по вопросам информационной (компьютерной) безопасности.

Следует подчеркнуть, что абсолютно надежной защиты компьютерной системы не существует и речь может идти лишь о степени ее надежности.

Причинами утери или искажения информации могут быть:

нарушение работы компьютера (кабельной системы, электропитания, дисков, системы архивирования данных, серверов, рабочих станций, сетевых карт, модемов);

повреждение носителей информации;

некорректная работа программного обеспечения вследствие ошибок или действия вредоносных программ типа вирусов и т.п.;

повреждение информации;

преступные действия злоумышленников, в частности, несанкционированный доступ с целью копирования, уничтожения, подделки информации;

неправильное хранение информационных архивов;

ошибки обслуживающего персонала и пользователей.

Рассмотрим некоторые приемы и методы, связанные с защитой информации от случайных ошибок или некомпетентности пользователей, а также от сбоев аппаратуры, в частности из-за помех в электросети, то есть причин возможной потери информации, не связанных с несанкционированным доступом и происками злоумышленников. Потеря файлов, а также крах системы вполне возможны и без внешних, корыстных помыслов. В связи с этим во всех операционных системах предусматриваются простейшие средства профилактики. Так при удалении файлов, как правило, требуется дополнительное подтверждение, а удаленный файл, как правило, при необходимости может быть восстановлен, поскольку определенное время он хранится в специальном буфере («корзина для мусора»).

Для того чтобы обезопасить себя от неприятных последствий (связанных с вышеперечисленными инцидентами), приводящих к потере данных на сервере или рабочих станциях, которые могут представлять большую ценность, так как являются результатом больших трудовых затрат, необходимо выполнение определенных мероприятий. Существует три основных способа защиты от таких воздействий — резервное копирование данных, избыточное дублирование и установка специализированных устройств защиты от нарушений в системе электропитания.

Резервное копирование данных

Методы, используемые для резервного копирования, зависят от их объема, важности информации и динамики ее изменения. Если говорить

о носителях, применимых для хранения резервных копий, то дискеты годятся лишь в частных случаях для небольших объемов информации и личных архивов пользователей. В большинстве случаев используются либо накопители на магнитной ленте (стримеры), либо магнитно-оптические устройства, либо оптические типа WORM или WARM. Независимо от типа устройства для резервного копирования необходимо систематически проводить копирование данных во избежание их потери. Выбор конкретного способа зависит от того, как часто изменяются данные, какую ценность они представляют и как много времени потребуется для этой процедуры. В настоящее время существуют следующие способы резервного копирования.

Случайный. При таком подходе производится случайное копирование отдельных файлов. Метод является наименее надежным, так как если обнаружится, что копия не самая новая, приходится проделать весь объем работы от момента изготовления этой резервной копии. Еще хуже, если носитель, на котором находится резервная копия, окажется поврежденным. Однако это лучше, чем ничего.

Серьезный. Резервные копии производятся регулярно и для их изготовления используются два набора носителей.

Профессиональный. Этот метод используют вычислительные центры с дорогостоящим оборудованием и большими компьютерами. В нем используются три копии данных на трех наборах носителей (для надежности иногда используются по два экземпляра для каждого из наборов). При работе поочередно используется каждый из наборов. Этот метод иногда называют схемой «сын — отец — дед».

Избыточность данных

Резервирование также подразумевает избыточность данных. С точки зрения подлинности, лучше иметь два среднего размера файловых сервера в локальной сети, чем один большой. Тогда в случае выхода из строя одного из них можно временно продолжать работать с другим. Конечно же, при этом на втором сервере должны находиться резервные копии рабочих файлов.

Несмотря на то, что системы хранения данных, основанные на магнитных дисках, производятся уже 40 лет, массовое производство отказоустойчивых систем началось совсем недавно. Дисковые массивы с избыточностью данных, которые принято называть RAID (redundant arrays of inexpensive disks — избыточный массив недорогих дисков, redundant array of independent disks — избыточный массив независимых дисков) были представлены исследователями (Петтерсон, Гибсон и Катц) из Калифорнийского университета в Беркли в 1987г. Но широкое распространение RAID системы получили только тогда, когда диски, которые подходят для использования в избыточных массивах, стали доступны и достаточно производительны. Со времени представления официального доклада о RAID в 1988г., исследования в сфере избыточных дисковых массивов начали бурно развиваться в попытке обеспечить широкий спектр решений на основе компромисса «цена — производительность — надежность». Производители файловых серверов, учитывая необходимость избыточности данных, предлагают модели с дисковыми массивами — системами НЖМД, в которых информация зеркально дублирована на различных дисководах. Естественно, что избыточность данных ни в коей мере не заменяет необходимость резервного копирования.

Защита от нарушений в системе электропитания

Рассмотрим теперь защиту от помех в электросети. Сбои электропитания всегда происходят неожиданно. В момент сбоя электросети практически любая программа может в какой-то степени испортить файл, с которым она работала. Для защиты от таких ситуаций необходимо использовать источники бесперебойного питания (UPS — Uninterruptible Power System) файл-серверов. Нет необходимости подключать к UPS рабочие станции, поскольку производители UPS нормируют их по максимальной мощности подключенных к ним приборов, так что не следует превышать эту величину.

После пропадания напряжения в электросети батареи UPS обеспечивают работоспособность сервера в последующие пять-десять минут — время, достаточное для того, чтобы завершить работу и успеть сохранить рабочие файлы. Кроме того, UPS защищает файл-сервер от скачков напряжения в электросети.

Существуют и более дешевые системы дежурного питания (SPS — Standby Power System) вместе с фильтром напряжения сети, которые защищают оборудование от кратковременных исчезновений электроэнергии в электросети, выбросов и помех.

На современных критически важных серверах принято за правило устанавливать особые «Redundant-блоки питания», которые предоставляют системному администратору возможность подключать сервер одновременно к двум источникам питания (например, к двум электрическим розеткам, подключенным к двум независимым электрическим группам, или одновременно к электрической розетке и к UPS). При падении напряжения на одном из подключений сервер продолжает работать на другом. Это намного повышает надежность питания сервера и позволяет производить плановую замену UPS без остановки сервера.

Заметим, что термины «информационная безопасность» (information security) и «безопасность сети» (network security) в широком смысле относятся к секретности, т.е. гарантии того, что информация и службы, имеющиеся в сети, не будут доступны для несанкционированного использования. Безопасность подразумевает механизм защиты, гарантирующий невозможность несанкционированного доступа к вычислительным ресурсам, шпионажа или перехвата сообщений, а также доступа в работу служб. Конечно, нельзя гарантировать абсолютную безопасность сети, так же как нельзя гарантировать полную защищенность материальных ценностей.

Обеспечение информационной безопасности требует охраны как физических, так и виртуальных ресурсов. К физическим устройствам можно отнести как пассивные устройства для хранения информации, такие как жесткие диски и компакт-диски, так и активные устройства,

такие как компьютеры пользователей. В сетевом окружении понятие физической безопасности относится к кабелям, мостам, маршрутизаторам и т.д. Хотя физическая безопасность упоминается очень редко, она часто играет важную роль при планировании полной безопасности, а меры по ее обеспечению достаточно традиционны и хорошо известны.

Обеспечение безопасности виртуального ресурса, такого как информация, обычно связывают с тремя основными понятиями компьютерной безопасности.

Угроза безопасности компьютерной системы — это потенциально возможное происшествие, которое может оказать нежелательное воздействие на саму систему, а также на информацию, хранящуюся в ней. Обычно выделяют три вида угроз:

угроза раскрытия заключается в том, что информация становится известной нежелательным лицам. Иногда вместо слова «раскрытие» используют термины «кража» или «утечка».

угроза целостности включает себя любое умышленное изменение (модификацию или даже удаление) данных, хранящихся в вычислительной системе или передаваемых из одной системы в другую. Обычно считается, что угрозе раскрытия подвержены в большей степени государственные структуры, а угрозе целостности — деловые или коммерческие.

угроза отказов обслуживания возможна всякий раз, когда в результате определенных действий блокируется доступ к некоторому ресурсу вычислительной системы. Блокирование может быть постоянным (чтобы запрашиваемый ресурс никогда не был получен) или может вызвать только задержку, достаточно долгую для того, чтобы он стал бесполезным. В таких случаях говорится, что ресурс исчерпан. В локальных вычислительных системах наиболее частыми являются угрозы раскрытия и целостности информации, а в глобальных на первое место выходит угроза отказа от обслуживания.

Уязвимость компьютерной системы — это некоторые ее неудачные характеристики, которые дают возможность возникновения угрозы. Именно из-за уязвимости в системе происходят нежелательные явления.

Атака на компьютерную систему — третье основополагающее понятие компьютерной безопасности. Это действие, предпринимаемое злоумышленником, которое заключается в поиске той или иной уязвимости. Таким образом, атака — реализация угрозы. К сетевым системам, наряду с обычными (локальными) системами, осуществляемыми в пределах одной компьютерной системы, применим специфический вид атак, обусловленный распределенностью ресурсов и информации в пространстве — так называемые «сетевые (или удаленные) атаки». Они характеризуются, во-первых, тем, что злоумышленник находится за тысячи километров от атакуемого объекта, и, во-вторых, тем, что нападению может подвергаться не конкретный компьютер, а информация, передающаяся по сетевым соединениям. С развитием локальных и глобальных сетей именно удаленные атаки считаются лидирующими по количеству попыток и по успешности их применения, поэтому обеспечение безопасности с точки зрения противостояния сетевым атакам приобретает первостепенное значение.

Под удаленной атакой обычно понимается информационное разрушающее воздействие на распределенную вычислительную систему, программно осуществляемое по каналам связи. Это определение охватывает как удаленные атаки на информационную инфраструктуру и протоколы сети, так и удаленные атаки на операционные системы и приложения. Под инфрастуктурой сети понимается как сложившаяся система организации связи между объектами сети, так и используемые в сети сервисные службы. А под операционными системами и приложениями — все программное обеспечение, работающее на удаленном компьютере, которое тем или иным образом обеспечивают сетевое взаимодействие.

Хотя понятие «информационная безопасность» охватывает множество способов защиты, основными из них являются следующие.

Безопасность целостности данных. Безопасная система должна защитить информацию от несанкционированного изменения и повреждения.

Доступность данных. Система должна гарантировать, что несанкционированный пользователь не может помешать законному доступу к данным.

Секретность и конфиденциальность. Система не должна позволять несанкционированным пользователям создавать копии данных во время их передачи по сети, а также анализировать их содержимое в том случае, если копии все-таки сделаны.

Авторизация. Меры информационной безопасности должны быть избирательными, учитывающими классификацию людей и ресурсов по различным категориям.

Аутентификация. Система должна позволять двум взаимодействующим между собой объектам проверить подлинность друг друга.

Запрещение повторного использования. Чтобы посторонние не могли перехватывать копии с целью их дальнейшего использования, система не должна обрабатывать копии повторно переданных пакетов данных.

Указывая основные понятия информационной безопасности, необходимо указать и правонарушителей, так или иначе связанных с проблемами компьютерного взлома, так называемых «хакеров». Общественное мнение специалистов в отношении деятельности хакеров неоднозначно, оно либо сугубо негативное (хакеры — это преступники), либо достаточно позитивное (хакеры — «санитары леса»). В действительности, эта деятельность имеет как положительную сторону, так и сугубо отрицательную, и эти две стороны четко разграничены. В связи с этим некоторые специалисты предлагают разделить всех профессионалов, связанных с информационной безопасностью, на хакеров (hackers) и кракеров (crackers). И те, и другие во многом занимаются решением одних и тех же задач — поиском уязвимости в вычислительных системах и осуществлением на них атак («взломом»).

Кракеры (crackers) — специалисты, способные снять защиту от копирования с лицензионного программного обеспечения. В современном компьютерном андеграунде кракерами обычно называют взломщиков программного обеспечения, в то время как хакерами именуют людей, специализирующихся на взломе защиты отдельных компьютеров и распределенных систем.

Принципиальное различие между хакерами и кракерами состоит в целях, которые они преследуют. Основная цель хакера состоит в том, чтобы исследуя вычислительную систему обнаруживать слабые места (уязвимость) в ее системе безопасности и информировать пользователя и разработчиков системы с целью устранения найденных уязвимостей. Другая задача хакера — проанализировать существующую систему, сформулировать необходимые требования и условия повышения уровня ее защищенности. Задача кракера состоит в непосредственном осуществлении взлома системы с целью получения несанкционированного доступа к чужой информации для кражи, подмены или объявления факта взлома. Среди основных целей кракеров следует отметить следующие:

получить доступ к важной информации, закрытой по тем или иным соображениям от использования посторонними лицами;

получить доступ к ресурсам чужой системы (процессору, внешней памяти и т.п.). В этом случае владелец системы ничего не теряет за исключением времени занятости процессора и части дискового пространства. Но, возможно, и приобретает достаточно дорогое программное обеспечение;

нарушить работоспособность хоста, без реализации угрозы раскрытия. Это может быть достаточно опасным, если хост обеспечивает бесперебойное обслуживание клиентов;

создать плацдарм для осуществления вышеназванных целей, но для атаки на другой компьютер с целью переадресовать корыстные цели на чужой компьютер;

отладить механизм атак на другие системы, используя атакованный компьютер в качестве пробного.

Мотивы кракеров низменны, но их состав неоднороден. Существует даже их классификация, в соответствии с которой кракеров разделяют на следующие категории:

1) вандалы — самая известная (благодаря распространению вирусов) и самая малочисленная часть кракеров. Их основная цель — взломать систему для ее дальнейшего разрушения. Это специалисты в написании вирусов и их разновидностей под названием «троянских коней». Эта стадия «кракерства» характерна для новичков и быстро проходит, если кракер продолжает совершенствоваться.

2) «шутники» — наиболее безобидная часть кракеров. Основная цель «шутников» — известность, достигаемая путем взлома компьютерных систем и внедрения туда различных эффектов, выражающих их неудовлетворенное чувств юмора. К «шутникам» также можно отнести создателей вирусов с различными визуально-звуковыми эффектами («музыкодрожание» или переворачивание экрана и т.п.) «Шутники», как правило, не наносят существенного ущерба компьютерным системам и администраторам. Все их действия — либо невинные шалости, либо рекламные акции профессионалов.

3) взломщики — профессиональные кракеры. Их основная задача — взлом компьютерной системы с серьезными целями, например, с целью кражи или подмены хранящейся в системе информации. Как правило, для того чтобы осуществить взлом, необходимо пройти три основные стадии:

исследование вычислительной системы с выявлением в ней изъянов (уязвимости);

разработку программной реализации атаки;

непосредственное осуществление атаки.

Настоящими профессионалом можно считать того кракера, который для достижения своей цели проходит все три стадии. В принципе, работа взломщиков — это обычное воровство. Однако в нашй стране, где находящееся у пользователей программное обеспечение в преобладающей части является пиратским, т.е. украденным не без помощи тех же взломщиков, отношение к ним не столь категорично.

В связи с этим, если не ограничиваться рассмотрением хакеров и кракеров с позиций распределенных систем, то следует отметить, что самая многочисленная категория кракеров занимается снятием защиты с коммерческих версий программных продуктов, изготовлением регистрационных ключей (registrationkey) для условно-бесплатных программ (shareware) и т.п.

Следует отметить, что в последнее время сформировался устойчивый миф о всемогуществе кракеров и хакеров и полной незащищенности компьютерных систем. Действительно, современные вычислительные системы общего назначения имеют серьезные проблемы с безопасностью. Но речь идет именно о системах общего назначения. Там же, где требуется обработка критической информации и обеспечение высшего уровня защиты (например, в военной области, атомной энергетике и т.п.), используются специализированные защищенные вычислительные системы, которые изолированы от сетей общего назначения физически и не допускают несанкционированного удаленного доступа извне. В то же самое время любая уважающая себя организация, будь то ЦРУ, АНБ, НАСА, имеет свои www- или FTP-серверы, находящиеся в открытой сети и доступные всем, и кракеры в этом случае проникали именно в них.

Другим, еще более устойчивым, является миф о всеобщей беззащитности банковских систем. Действительно, в отличие от вычислительных систем стратегического назначения, банки вынуждены для обеспечения удобства и оперативности работы с клиентами предоставлять им возможность удаленного доступа из сетей общего пользования к своим банковским вычислительным системам. Однако для связи в этом случае используются защищенные криптопротоколы и разнообразные системы сетевой защиты, и к тому же предоставление клиенту возможности удаленного доступа отнюдь не означает, что клиент может получить доступ непосредственно к внутренней банковской сети.

По мнению специалистов, зарубежные банковские вычислительные системы являются наиболее защищенными вслед за системами

стратегического назначения. В обоих случаях речь идет о несанкционированном удаленном доступе извне. В том случае, если нанести ущерб системам вознамерится кракер из состава персонала защищенной системы, трудно судить об успехе его попыток. Как утверждают статистики, нарушение безопасности системы собственным персоналом составляет около 90% от общего числа нарушений. Таким образом, даже критические вычислительные системы нельзя считать неуязвимыми, но реализовать на них успешную удаленную атаку практически невозможно.

Как утверждают некоторые исследователи, ни одного подтвержденного факта целенаправленного взлома с помощью программных средств (а не с помощью подкупа и т.п.) указанных выше систем ни в России, ни за рубежом пока обнаружить не удалось.

Рассмотрим теперь некоторые меры защиты от удаленных атак. Следует отметить, что защита от удаленных атак взаимосвязана с методами доступа и использованными пользователем ресурсами глобальной сети. Сети являются общедоступными. Удаленный доступ к этим ресурсам может осуществляться анонимно любым неавторизованным пользователем. Примером неавторизованного доступа является подключение к www- или FTP-серверам. В этом случае, если трафик пользователя будет перехвачен, пройдет через сегмент атакующего, то последний не получит ничего, кроме общедоступной информации, т.е. отпадает забота о защите информации. Если же планируется авторизованный доступ к удаленным ресурсам, то следует обратить на эту проблему особое внимание.

Методы защиты связаны также с используемой пользователем операционной системой. При этом имеется в виду: собирается ли пользователь разрешать удаленный доступ из сети к своим ресурсам. Если нет, то пользователь должен использовать чисто «клиентскую» операционную систему (например, Windows или NT Workstation). Удаленный доступ к данной системе в принципе невозможен, что, безусловно, повышает ее безопасность (хотя и не гарантирует ее полностью). Естественно, все ограничения, связанные с безопасностью,

ухудшают функциональность системы. В связи с этим существует такая «аксиома безопасности»: «Принципы доступности, удобства, быстродействия и функциональности вычислительной системы антагонистичны принципам ее безопасности. Чем более удобна, быстра и многофункциональна вычислительная система, тем она менее безопасна». Естественно, полная изоляция компьютера от глобальной сети путем отключения разъема или создания выделенной линии связи обеспечивает абсолютную безопасность от удаленных атак, однако полностью исключает функциональные возможности сетей и поэтому бессмысленна. Основная же цель комплексной защиты информации — обеспечение максимальных функциональных возможностей при максимальной защищенности сети. Среди разнообразных мер по защите от удаленных атак наиболее простыми и дешевыми являются административные меры. Например, как можно защититься от анализа сетевого трафика злоумышленником, если известно, что с помощью программного прослушивания можно перехватить любую информацию, которой обмениваются удаленные пользователи, когда по каналу передаются нешифрованные сообщения? Также известно, что базовые прикладные протоколы удаленного доступа TELNET и FTP не предусматривают элементарную защиту передаваемых по сети идентификаторов (имен) и аутентификаторов (паролей).

Поэтому администраторы сетей могут запретить использовать эти базовые протоколы для предоставления авторизованного доступа к ресурсам своих систем. При необходимости можно рекомендовать средства защиты этих протоколов.

Определенную опасность представляет использование так называемого протокола ARP. Этот протокол осуществляет поиск и сопоставление IP адреса с адресом конкретной локальной сети (например, Ethernet) и направление следования именно по этому адресу. Перехваченный IP пакет может быть в данном случае направлен по ложному адресу (по ложному ARP серверу). Чтобы устранить эту неприятность, связанную с отсутствием у операционной системы каждого хоста необходимой информации о соответствующих IP и Ethernet адресах

остальных хостов внутри данного сегмента сети, сетевой администратор создает статическую ARP таблицу в виде файла, куда вносится необходимая информация об адресах. Данный файл устанавливается на каждый хост внутри сетевого сегмента, и, следовательно, у сетевой операционной системы отпадает необходимость использования удаленного ARP поиска.

Известна также уязвимость адресной службы DNS, что позволяет кракеру получить глобальный контроль над соединениями путем навязывания ложного маршрута через хост кракера — ложный DNS сервер. Это приводит к катастрофическим последствиям для огромного числа пользователей. Защита от ложного DNS сервера — достаточно сложная задача, однако и в этом случае могут быть предложены административные методы, которые могут предотвратить установление такого глобального контроля либо защитить подобную удаленную систему. Разработаны административные меры от навязывания ложного маршрута, защиты от отказа в обслуживании и от других причин нарушения безопасности информации.

Признавая важность административных мер защиты от удаленных атак, тем не менее, следует считать, что основную роль играют все же программно-аппаратные методы защиты. Центральным элементом в комплексе программно-аппаратных методов является криптография. В течение многих лет криптография использовалась исключительно в военных целях. В последние 20—30 лет наблюдается быстрый рост несекретных академических исследований в области криптографии. Сегодня современная компьютерная криптография широко практикуется и вне военных ведомств, что, безусловно, связано с расширением сфер деятельности пользователей, в которых возникает потребность в криптографических методах защиты информации. Это научное направление имеет серьезное теоретическое (математическое, алгоритмическое) обоснование. В открытой печати уже появилось много публикаций, учебников и солидных монографий по криптографии.

Конкретная реализация методов криптографии связана с разработкой аппаратных и программных средств, так, например,

мейнфреймы фирмы IBM начиная с 90х гг. прошлого века (1990) оснащаются криптографическими процессорами, обеспечивающими шифрование и дешифрование сообщений с минимальной дополнительной нагрузкой на центральный процессор. Эти спецпроцессоры могут обрабатывать большие объемы данных и обеспечивать высокий уровень защищенности вычислительных систем. Важную роль в реализации криптографических методов играет разработка генераторов «истинно случайных» чисел и другие исследования.

В качестве примера применения криптографических методов рассмотрим процедуру защиты IP протокола в глобальной сети Интернет. Обеспечить безопасность глобальной сети Интернет особенно трудно, поскольку дейтаграммы, передающиеся от отправителя до конечного получателя, проходят через несколько промежуточных сетей и маршрутизаторов, не контролируемых ни отправителем, ни получателем. Таким образом, поскольку дейтаграммы могут быть перехвачены без ведома отправителя, их содержимому нельзя доверять. Например, рассмотрим сервер, который использует процедуру аутентификации источника для проверки того, что запросы поступают от авторизованных клиентов. Процедура аутентификации источника требует, чтобы сервер при получении каждой дейтаграммы проверял IP адрес отправителя и принимал запросы только от компьютеров, адреса которых перечислены в специальном списке. Данный вид аутентификации обеспечивает слабую защиту, поскольку ее можно легко обойти. В частности, один из промежуточных маршрутизаторов может контролировать трафик проходящих через него дейтаграмм и фиксировать IP адреса авторизованных клиентов, которые могут быть перехвачены любым злоумышленником, контролирующим этот маршрутизатор. Затем этот злоумышленник может выступить в роли авторизованного клиента.

Группа IETF (Internet Engineering Task Forse) — инженерная группа, входящая в структуру архитектурного совета Интернет, разработала набор протоколов, которые обеспечивают безопасную связь в глобальной сети. Все вместе они называются семейством протоколов

IPsec (IP security или защитным протоколом IP). В этих протоколах аутентификация и шифрование данных выполняются на уровне протокола IP.

Методы криптографии, применяемые при разработке разнообразных криптопротоколов, составляют основу программных методов защиты информации в сетях. В то же время они являются составной частью так называемой методики Firewall, являющейся сейчас основой программно-аппаратных средств осуществления сетевой политики безопасности в IP сетях и реализующей следующие функции:

Многоуровневая фильтрация сетевого трафика. Фильтрация обычно происходит на четырех уровнях OSI:

канальном (Ethernet),

сетевом (IP),

транспортном (TCP, UDP),

прикладном (FTP, TELNET, HTTP, SMTP и т.д.).

Фильтрация сетевого трафика является основной функцией системы Firewall и позволяет администратору безопасности сети централизованно осуществлять необходимую сетевую политику в выделенном сегменте IP сети. Настроив для этого соответствующим образом Firewall, можно разрешить или запретить пользователям как доступ из внешней сети к соответствующим службам хостов или к хостам, находящимся в защищенном сегменте, так и доступ пользователей из внутренней сети к соответствующим ресурсам внешней сети.

Proxy — схема с дополнительной идентификацией и аутентификацией пользователей. Смысл proxy-схемы заключается в создании соединения с конечным адресатом через промежуточный сервер, называемый proxy-сервером (proxy — полномочный), на хосте Firewall.

Создание приватных сетей с виртуальными IP адресами. Если администратор безопасности считает целесообразным скрыть истинную топологию своей внутренней IP сети, он может использовать proxy-сервер для отделения своей внутренней приватной сети со своими

внутренними виртуальными IP адресами, которые, очевидно, непригодны для внешней адресации. При этом proxy-сервер должен осуществлять связь с абонентами из внешней сети со своего настоящего IP адреса. Эти же схемы применяются и в том случае, если для создания IP сети выделено недостаточное количество IP адресов. Основным аппаратным компонентом для реализации методики управления доступом к объединенной сети является специализированное устройство, называемое брандмауэром, ассоциируемое с термином Firewall (термин брандмауэр позаимствован из строительства, где он обозначает толстую несгораемую стену, благодаря которой секция строения становится непроницаемой для огня). Обычно «брандмауэр» устанавливается между внутренней сетью организации и каналом, ведущим к внешним сетям (например, к глобальной сети Интернет). Брандмауэры разделяют объединенную сеть на две области, которые неофициально называются внутренней и внешней. Хотя сама идея брандмауэра проста, ее реализация усложняется множеством факторов. Один из них — внутренняя сеть организации может иметь несколько внешних соединений. При этом необходимо сформировать периметр безопасности (security perimeter), установив брандмауэр на каждое внешнее соединение. Чтобы гарантировать эффективность периметра безопасности, во всех брандмауэрах должны использоваться одинаковые ограничения доступа. В противном случае злоумышленники могут обойти ограничения, наложенные одним брандмауэром, и зайти в объединенную сеть через другой.

Существует несколько способов реализации брандмауэров. Выбор способа зависит от того, какое количество внешних каналов существует в организации. В большинстве случаев каждый барьер в брандмауэре реализуется на основе маршрутизатора, содержащего фильтр пакетов. Чтобы брандмауэр не замедлял работу сети, его аппаратное и программное обеспечение должно быть оптимизировано на решение конкретной задачи. Решению этой задачи способствует и тот факт, что в большинство коммерческих маршрутизаторов включен

быстродействующий механизм фильтрации пакетов, который выполняет основную часть работы.

На практике, как правило, возникает необходимость создать безопасный брандмауэр, который предотвратит нежелательный доступ извне и в то же время позволит пользователям внутренней сети получить доступ к внешним службам. При этом необходимо выработать специальный механизм безопасности. В общем случае организация может обеспечить доступ к внешним службам только через защищенный компьютер. Поэтому обычно с каждым брандмауэром связывают один защищенный компьютер и устанавливают на этом компьютере набор шлюзов уровня приложения. Для того чтобы такой компьютер мог служить в качестве безопасного канала связи, его степень защиты должна быть очень высока. Поэтому такой компьютер часто называют бастионным узлом. На бастионном узле запускаются службы, которые организация хочет сделать видимыми извне, а также proxy-серверы, которые позволяют внутренней сети получить доступ к внешним серверам. В брандмауэре также может использоваться так называемая «тупиковая сеть», которая позволяет изолировать внешний трафик от внутреннего. К этой сети подключаются брандмауэры, а также бастионный узел.

Все брандмауэры можно разделить на три типа:

1) пакетные фильтры (packet filter);

2) серверы прикладного уровня (application gateways);

3) серверы уровня соединения (circuit gateways).

Все типы могут одновременно встретиться в одном брандмауэре.

Пакетные фильтры

Брандмауэры с пакетными фильтрами принимают решение о том, пропускать пакет или отбросить, просматривая IP адреса, флажки или номера TCP портов в заголовке этого пакета. IP адрес и номер порта — это информация сетевого и транспортного уровней соответственно, но пакетные фильтры используют и информацию прикладного уровня, так

как все стандартные сервисы в TCP/IP ассоциируются с определенным номером порта.

Серверы прикладного уровня

Брандмауэры с серверами прикладного уровня используют серверы конкретных сервисов — TELNET, FTP и т.д. (proxy server), запускаемые на брандмауэре и пропускающие через себя весь трафик, относящийся к данному сервису. Таким образом, между клиентом и сервером образуются два соединения: от клиента до брандмауэра и от брандмауэра до места назначения. Использование серверов прикладного уровня позволяет решить важную задачу — скрыть от внешних пользователей структуру локальной сети, включая информацию в заголовках почтовых пакетов или службы доменных имен (DNS). Другим положительным качеством является возможность аутентификации на пользовательском уровне.

При описании правил доступа используются такие параметры, как название сервиса, имя пользователя, допустимый временной диапазон использования сервиса, компьютеры, с которых можно пользоваться сервисом, схемы аутентификации. Серверы протоколов прикладного уровня позволяют обеспечить наиболее высокий уровень защиты — взаимодействие с внешним миром реализуется через небольшое число прикладных программ, полностью контролирующих весь входящий и выходящий трафик.

Серверы уровня соединения

Сервер уровня соединения представляет собой транслятор TCP соединения. Пользователь образует соединение с определенным портом на брандмауэре, после чего последний производит соединение с местом назначения по другую сторону от брандмауэра. Во время сеанса этот транслятор копирует байты в обоих направлениях, действуя как провод. Как правило, пункт назначения задается заранее, тогда как источников

может быть много (соединение типа «один со многими»). Используя различные порты, можно создавать различные конфигурации. Такой тип сервера позволяет создавать транслятор для любого определенного пользователем сервиса, базирующегося на TCP, осуществлять контроль доступа к этому сервису, сбор статистики по его использованию.

Относительно программных средств защиты информации необходимо отметить, что конечной целью атаки кракера является определенный компьютер, с конкретной реализацией сетевых протоколов, с конкретной определенной системой. В связи с этим необходимо коснуться защиты операционных систем. Среди типичных атак, которым могут быть подвергнуты любые ОС, можно указать следующие:

кража пароля (подглядывание за несколькими пользователями, получение из файла, кража носителей и т.п.);

подбор пароля (перебор возможных вариантов, включая оптимизированный перебор);

копирование «жестких» дисков компьютера;

сбор «мусора»: если средства операционной системы позволяют восстанавливать ранее удаленные объекты, злоумышленник может получить доступ к удаленным объектам (удаленным другими пользователями), просмотрев содержимое их мусорных корзин;

превышение полномочий: используя ошибки в программном обеспечении или администрировании операционной системы, злоумышленник получает полномочия, превышающие те, которые предоставлены ему согласно действующей политике безопасности;

отказ в обслуживании (целью этой атаки является частичный или полный вывод операционной системы из строя, как правило, с помощью вирусов).

Самой распространенной операционной системой в глобальной сети Интернет является операционная система Unix, основными протокольными определяющими сети Интернет являются протоколы TCP/IP, которые были разработаны для системы Unix. Не менее 90% мощных Интернет-узлов работают под управлением этой системы и

различных ее диалектов. Основные концепции Unix разрабатывались в конце 60-х — начале 70-х гг. прошлого столетия, когда не было никакой теории компьютерной безопасности и никто не подозревал о тех крупных неприятностях, которые возникнут по мере развития сетевых технологий. Современные сетевые операционные системы оказываются в заведомо более выгодном положении, поскольку они разрабатывались с учетом ошибок Unix и современной ситуации с безопасностью сетей. Однако это вовсе не говорит об их большей безопасности.

За долгий срок жизни Unix исследователями написаны, а администраторами изучены сотни статей и книг относительно механизмов безопасности Unix и способов их нарушения. Все это позволяет предположить, что никаких сюрпризов Unix больше не преподнесет.

С новыми операционными системами ситуация прямо противоположная. И хотя в них заложены концепции, согласующиеся с современным состоянием теории безопасности, у них очень малый срок эксплуатации. Они активно исследуются хакерами и кракерами, и, несмотря на опыт Unix, начинают проходить тот же самый путь и совершать те же самые ошибки в обеспечении безопасности.

В дополнение следует добавить несколько замечаний о структуре средств информационной безопасности операционной системы Unix и наиболее слабых ее местах. Как известно, изначально система Unix была ориентирована на централизованные вычисления в системах коллективного пользования как многозадачная, многопользовательская система. Пользователи системы разделялись на группы, в зависимости от прав доступа (или привилегий):

суперпользователь (root), имеющий неограниченные права;

обычный пользователь, имеющий права в рамках своего идентификатора (UID, user ID);

членство в группе (GID, group ID) — права и ограничения устанавливаются для него суперпользователем.

По мере развития операционной системы и использования Unix-машин в качестве серверов в глобальных сетях среди обычных

пользователей выделялись так называемые специальные пользователи. Они, как правило, имеют зарегистрированные имена (guest, bin, uucp и т.п.) и номера UID и GID. Прав у этого пользователя еще меньше, чем у обычного. Их устанавливает суперпользователь для работы с конкретными приложениями. Одним из интересных примеров специального пользователя является анонимный пользователь FTP, который так и называется anonymous, или ftp.

И, наконец, есть категория так называемых псевдопользователей, не имеющих никаких прав и не идентифицируемых системой. Но они могут подключаться к системе с помощью так называемых программ-демонов (в современной терминологии серверов), в частности, используя средства электронной почты e-mail. От этого пользователя не требуется аутентификации, учет по нему также не ведется.

Именно две последние категории пользователей (особенно последняя) и являются причиной основных неприятностей в операционной системе Unix с точки зрения информационной безопасности. Среди основных причин уязвимости Unix принято считать:

наличие доменов;

механизм SUID/SGIN — это атрибут, который предоставляет право иметь привилегии суперпользователя, в частности, возможность смены идентификатора (собственного пароля);

излишнее доверие, поскольку в не столь давние времена создатели делали систему «под себя», не подозревая, насколько теснее и опаснее станет компьютерный мир через несколько лет.

Также слабым местом Unix-систем являются «люки». «Люком» или «черным входом» (backdoor) часто называют оставленную разработчиком недокументированную возможность взаимодействия с системой (чаще всего — входа в нее), например, известный только разработчику универсальный пароль. Люки оставляют в конечных программах вследствие ошибки, не убрав отладочный код, или вследствие необходимости продолжения отладки уже в реальной системе из-за ее высокой сложности, или же из корыстных интересов.

Учитывая динамику развития операционной системы Unix, в настоящее время можно сказать, что она является наиболее мощной и надежной, в том числе и со стороны информационной безопасности системы.

Рассмотрим, наконец, методы цифровой подписи данных, передаваемых в сетях, т.е. защиту документов, скрепленных подписью ответственного лица, называемых «электронной подписью».

Подпись «от руки» издавна используется для доказательства авторских прав или согласия с документом. Из наиболее важных аспектов подписи отметим следующие:

подпись достоверна; она убеждает получателя, что человек, подписавший документ, сделал это сознательно;

подпись не поддельна; она доказывает, что именно указанный человек подписал документ;

подпись невозможно использовать повторно, она составляет часть документа, ее невозможно нанести на другой документ;

подписанный документ невозможно изменить;

от подписи нельзя отказаться.

Хотя все эти утверждения не бесспорны, однако действия мошенников с традиционно подписанными документами затруднены и они рискуют быть разоблаченными.

Однако реализация электронной подписи и передача ее в сетях требует специальных мер защиты, так как ситуация оказывается гораздо сложнее. Во-первых, компьютерные файлы очень легко копируются. Даже если подпись человека или графическое изображение подписи от руки подделать нелегко, можно без труда «вырезать» подлинную подпись из этого документа и вставить ее в другой документ. Таким образом, простое наличие в документе такой подписи ничего не означает. Во-вторых, компьютерные файлы очень легко изменить уже после подписания документа, не оставив ни малейшего следа изменения.

В связи с этим механизм цифровой (электронной) подписи, реализуемый криптографическими методами, состоит из двух процессов:

1) формирования подписи блока данных при передаче;

2) проверки подписей в принятом блоке данных.

Первый процесс заключается в формировании подписи по определенному алгоритму с использованием секретного ключа. Второй — в обратном преобразовании.

Существует большое разнообразие криптографических протоколов для передачи цифровой подписи в сетях. Это и так называемые симметричные протоколы, когда ключ для шифрования сообщения аналогичен ключу для его прочтения, симметричные алгоритмы с посредником-арбитром и т.п. Считается, что для реализации цифровой подписи предпочтительнее методы шифрования с открытым ключом. В этом протоколе используется два ключа. Один — открытый (известный пользователям) и другой — закрытый (секретный). Используя открытый ключ, кто угодно может зашифровывать сообщение, но расшифровать сообщение может только владелец закрытого ключа. Одним из основных достоинств этого протокола является то, что вычислительными методами очень трудно определить закрытый ключ по открытому. Очень удачной аналогией этого протокола является почтовый ящик. Шифрование открытым ключом аналогично опусканию письма в почтовый ящик — это может сделать кто угодно, просто открыв паз и опустив в него письмо. Дешифрование с закрытым ключом при этом подобно извлечению почты из почтового ящика. Открыть его гораздо сложнее. Однако если у Вас есть ключи от почтового ящика, извлечь письмо нетрудно. Этот протокол является самодостаточным, так как для его выполнения не требуется ни посредник, ни арбитр для различения разногласий (как это имеет место в симметричных протоколах). Однако и этот протокол имеет недостатки.

Одним из самых ранних примеров использования цифровых подписей было упрощение проверки соблюдения договоров о ядерных испытаниях. Соединенные Штаты и Советский Союз разрешили друг другу разместить за границей сейсмографы для мониторинга ядерных испытаний. Проблема заключалась в том, что каждая сторона хотела быть уверенной, что страна, в которой размещены приборы, не подделывает их показаний. В свою очередь страна, в которой размещались сейсмографы, искала гарантий, что приборы посылают

только ту информацию, которая нужна для мониторинга испытаний. Эти проблемы были решены с помощью цифровых подписей. Сторона, на территории которой стоял сейсмограф, может читать, но не изменять данные сейсмографа, и наблюдающая сторона знает, что данные не подделываются.

Таким образом, комбинируя цифровые подписи и криптографию открытым ключом, можно создать протокол, сочетающий надежное шифрование с достоверностью цифровых подписей.

На рынке достаточно много предложений средств защиты Интернета, однако по ряду параметров ни одно из них не может быть признано адекватным задачам защиты информации именно для Интернета. Например, достаточно криптостойкой и замечательной по своей идее является распространенная система PGP (Pritty good privacy). Однако, поскольку PGP обеспечивает шифрование файлов, она применима только там, где можно обойтись файловым обменом. Защитить, например, приложения «on-line» при помощи PGP затруднительно. Кроме того, уровень иерархии управления защиты PGP слишком высок: эту систему можно отнести к прикладному или представительскому уровням модели OSI. Стыковка защиты PGP с другими прикладными системами потребует также определенных усилий, если, конечно, вообще окажется осуществимой. Альтернативу таким «высокоуровневым» системам защиты среди традиционных решений составляют устройства защиты канального и физического уровня — скремблеры и канальные шифраторы. Они «невидимы» с прикладного уровня и, в этом смысле, совместимы со всеми приложениями. Однако такие системы имеют ограниченную совместимость с различным каналообразующим оборудованием и физическими средами передачи данных. Это, как правило, не сетевые устройства, способные распознавать топологию сети и обеспечить связь из конца в конец через многие промежуточные узлы, а «двухточечные» системы, работающие на концах защищаемой линии и поэтому вносящие значительную аппаратную избыточность. И, конечно же, на таких устройствах невозможно построить систему защиты в рамках такой сети, как

Интернет, уже хотя бы потому, что невозможно обеспечить их повсеместное распространение (вследствие высокой цены) и всеобщую аппаратную совместимость.

В заключение обсуждения методов защиты информации следует отметить, что персонал представляет собой наиболее уязвимое звено в любой системе безопасности. Служащий фирмы либо по злому умыслу, либо по неосторожности, либо не зная принятой в организации стратегии, может поставить под угрозу самую современную систему безопасности. В изучении методов защиты информации сложилось даже целое направление — социальная инженерия, связанная со злоупотреблением доверием пользователей, например, как одним из наиболее эффективных методов получения информации у ничего не подозревающих сотрудников, особенно в больших организациях, где многие пользователи не знают персонал своих компьютерных подразделений «в лицо», общаясь, в основном, по телефону. По определению самих хакеров, «социальная инженерия» — это термин, используемый взломщиками и хакерами для обозначения несанкционированного доступа иным способом, чем взлом программного обеспечения; цель — обмануть сотрудников для получения паролей к системе или иной информации, которая поможет нарушить безопасность системы. Классическое мошенничество включает звонки по телефону, электронную почту, разговоры по Интернет в «реальном времени», обыкновенную почту, личные встречи и т.п.

Наиболее известную угрозу информационной безопасности представляют компьютерные вирусы.

Проблема «вирусов» и «вирусной безопасности» возникла достаточно давно. Первое исследование саморазмножающихся искусственных технических и программных конструкций проводились в середине прошлого столетия в работах фон Неймана, Винера и других ученых. Было дано определение и проведен математический анализ конечных автоматов, в том числе и самовоспроизводящихся. Термин «компьютерный вирус» появился позднее — официально считается, что его впервые употребил сотрудник Лехайского университета (США) Фред

Коэн в 1984г. на Седьмой конференции по безопасности информации, проходившей в США. Идеи вирусов были изложены широкой публике еще в 1983 году известным разработчиком ОС Unix Кэном Томпсоном в одной из своих лекций.

Одной из самых известных практических реализаций чисто теоретических работ фон Неймана и других известных ученых явилась программа Worm («червь»), созданная осенью 1988 г. студентом выпускного курса Корнелльского университета Робертом Морисом, который занимался в Bell Laboratories программным обеспечением безопасности Unix. Запущенный на сетевой машине «червь» искал в сети Интернет-машины с серверами и использовал их для воссоздания себя в большом количестве копий. Такое действие «червя» стало возможным в результате использования ошибки в программе («демоне») Unix fingered. Вирус распространялся с поразительной скоростью и появлялся в самых различных районах США. Через пять часов было поражено пять систем, через двое суток — шесть тысяч. По самым скромным оценкам вирус Мориса стоил свыше 8 миллионов часов потери доступа и свыше миллиона часов прямых потерь на восстановление работоспособности систем. Общая стоимость этих затрат оценивается в 98 миллионов долларов. Ущерб был бы еще большим, если бы вирус изначально создавался с разрушительными целями.

Этот крупнейший инцидент в области компьютерной безопасности доказал (не теоретически, а практически) возможность создания саморепродуцирующихся программ, дал толчок к появлению целой отрасли компьютерной безопасности — компьютерной вирусологии, а также выявил необходимость разработчиков Unix более серьезно заняться безопасностью этой операционной системы. К тому времени уже существовали единичные вирусы и на персональных компьютерах — саморепродуцирующиеся в пределах одного компьютера (видимо поэтому сетевые вирусы стали называться «червями»).

Так что же такое компьютерный вирус? По определению, данному одним из известных отечественных специалистов Евгением Касперским, компьютерным вирусом называется программа, которая может создавать

свои копии и внедряться в файлы и системные области компьютера, вычислительной сети и т.п. При этом копии сохраняют способность дальнейшего распространения. Другими словами, компьютерный вирус — небольшая программа (средний размер — 700 байт), написанная на языке Assembler и выполняющая разрушительные для операционной системы действия. Следует отметить, что такие программы как «бомбы» и «троянские кони» также приводят к неприятностям в системах, но отличаются от вирусов, так как не обладают свойством саморазмножения.

Название «вирус» распространилось ввиду явного сходства с биологическим прототипом. Суть воздействия биологического вируса сводится к нарушению информации, содержащейся в генетическом коде клетки. Посредством небольшого изменения фрагмента ДНК и РНК он захватывает управление жизненным процессом клетки. Таким образом, вирус обеспечивает себе возможность свободно и неограниченно размножаться. Это часто приводит к трагическим последствиям. Если компьютерную систему сопоставить с живым организмом, а отдельные программы — с клетками, то получим полную аналогию. Компьютерный вирус разрушает информацию, содержащуюся в коде программы. Он перехватывает контроль над компьютерной системой путем замены небольшого фрагмента программы, что позволяет ему неограниченно размножать свой код. Так же, как и биологический аналог, компьютерные вирусы:

представляют опасность для той системы, на которой они паразитируют;

быстро размножаются, легко распространяются на большие расстояния;

проявляют себя не сразу;

заболевание предшествует «латентный период», во время которого вирус продолжает распространяться в компьютерной системе;

важную роль в борьбе с «заболеваниями» играют профилактика и просвещение.

Биологическая аналогия оказывается настолько глубокой, что в литературе, посвященной компьютерным вирусам, широко используются и другие медицинские термины: «заболевание», «вакцина», «лечение», «карантин» и др., что иногда приводит к недоразумениям, когда забывается, что компьютерный вирус является обычной программой для компьютерной системы, которая имеет своего создателя.

Вирусы можно разделить на классы по следующим признакам:

по среде обитания вируса;

по способу заражения среды обитания;

по деструктивным возможностям.

По среде обитания различают, прежде всего, сетевые вирусы, или вирусы-черви (worm), которые распространяются в компьютерной сети. Проникая в память компьютера, они вычисляют сетевые адреса других машин и по этим адресам рассылают свои копии.

Файловые вирусы являются наиболее распространенным типом и обладают наибольшей инфицирующей способностью. Объектом поражения файловых вирусов являются исполняемые файлы, драйверы устройств и файлы операционной системы. По способу заражения файловые вирусы делятся на резидентные и нерезидентные.

Нерезидентный файловый вирус при запуске пораженной программы ищет первую «жертву» — незараженный файл в текущей директории и дописывает к ней свое тело, а затем передает управление запущенной программе. Нерезидентные вирусы не заражают память компьютера и сохраняют активность ограниченное время.

Резидентные вирусы находятся в памяти компьютера, оставляя в оперативной памяти свою резидентную часть, которая перехватывает обращение операционной системы к объектам заражения и внедряется в них. Резидентные вирусы находятся в памяти и остаются активными вплоть до выключения компьютера или его перезагрузки.

Загрузочные вирусы внедряются в загрузочный сектор системного диска, проникая в компьютер при загрузке зараженной дискеты. При идентификации диска вирус в большинстве случаев переносит

оригинальный boot-сектор в какой-либо другой сектор диска, а сам записывается на его место. В результате при загрузке с зараженного диска вместо настоящего boot-сектора будет выполнен программный код вируса, который при первой возможности делает свое «черное дело». В настоящее время этот вид вирусов обречен, так как практически все машины имеют защиту boot-сектора.

Вирусы всех типов могут распространяться по сети. По своим деструктивным возможностям «троянский» компонент вируса обычно разделяют на:

безвредные, никак не влияющие на работу компьютера, кроме изменения свободной памяти на диске в результате своего размножения;

неопасные, влияние которых ограничивается уменьшением объема свободной памяти на диске и графическими, звуковыми и прочими эффектами, к которым относится, например, выдача букв или проигрывание какой-нибудь мелодии в определенное время;

опасные вирусы, которые могут привести к серьезным сбоям в работе компьютера

очень опасные вирусы, которые могут привести к потере программ; уничтожить данные; стереть необходимую для работы компьютера информацию, записанную в системных областях памяти, и даже способствовать ускоренному износу движущихся частей диска.

Вирусы-«черви» (worm) — это вирусы, которые распространяются в компьютерной сети и так же, как и вирусы-«спутники», не изменяют файлы или секторы на дисках. Они проникают в память компьютера из компьютерной сети, вычисляют сетевые адреса других компьютеров и рассылают по этим адресам свои копии. Такие вирусы иногда создают рабочие файлы на дисках системы, но могут вообще не обращаться к ресурсам компьютера (за исключением оперативной памяти).

Отметим еще макровирусы. Это особая разновидность вирусов, которые поражают документы в прикладных программах, имеющие расширение .doc, например, документы, созданные текстовым процессором MS Word, и выполняющие макрокоманды. Если открыть файл документа в окне, происходит заражение.

Наиболее опасными в настоящее время представляются полиморфные вирусы — вирусы, модифицирующие свой код в зараженных программах таким образом, что два экземпляра одного и того же вируса могут не совпадать ни в одном бите. Такие вирусы не только шифруют свой код, используя различные способы шифрования, но и содержат код генерации шифровщика и расшифровщика, что отличает их от обычных шифровальных вирусов с постоянными кодами шифровальщика и дешифровщика. Полиморфные вирусы — это вирусы с самомодифицирующимися расшифровщиками. При таком шифровании, даже имея зараженный и оригинальный файлы, невозможно проанализировать код вируса обычными методами. Этот код зашифрован и представляет собой бессмысленный набор команд. Расшифровка производится самим вирусом непосредственно во время выполнения. При этом вирус может расшифровать себя всего сразу, а может выполнять расшифровку в ходе работы, вновь шифруя уже отработавшие участки с целью затруднения анализа кода вируса.

Абсолютных гарантий антивирусной безопасности не имеется, даже при наличии самых наилучших антивирусных программ. Однако путем соблюдения определенных правил профилактики (так называемой компьютерной гигиены), можно снизить до минимума риск заражения компьютеров.

Необходимо регулярно делать резервные копии файлов, с которыми ведется работа, на внешний носитель.

Следует покупать дистрибутивные копии программного обеспечения только у официальных продавцов.

Не следует запускать непроверенные антивирусные программы, полученные из сомнительных источников.

При лечении дисков следует использовать заведомо «чистую» операционную систему.

Необходимо иметь в виду, что очень часто вирусы переносятся с игровыми программами, с которыми следует быть предельно осторожным. В заключение следует отметить, что кроме вирусов существует другой вид программ, представляющих опасность для

вычислительных систем, о которых ранее упоминалось. Это так называемые «троянские» программы. Такие программы не способны самостоятельно размножаться, и их распространение основано целиком на добровольном копировании. При запуске такой программы она, выполняя внешне безобидные действия, одновременно портит данные в компьютере. «Троянские программы» распространяются значительно медленнее, чем вирусы, поскольку уничтожив систему они погибают сами. Как правило, их маскируют под игровые программы или широко известные пакеты.

8. Правовая система «Гарант»

В ст. 24 Закона «О средствах массовой информации» указано: «правила, установленные настоящим Законом для периодических печатных изданий, применяются в отношении периодического распространения тиражом тысяча и более экземпляров текстов, созданных с помощью компьютеров и(или) хранящихся в их банках и базах данных, а равно в отношении иных средств массовой информации, продукция которых распространяется в виде печатных сообщений, материалов, изображений». В соответствии с названным Законом СПС «Гарант» зарегистрирована в качестве средства массовой информации Министерством Российской Федерации по делам печати, телерадиовещания и средств массовых коммуникаций. Регистрация «Системы Гарант», как электронного периодического справочника, подтверждена свидетельством Эл № 77-2137 от 03.12.1999г.

Информационные ресурсы СПС «Гарант» составляют свыше 2 млн. документов и несколько гигабайт дополнительной экономической информации. Всего в СПС имеются четыре группы ресурсов:

1) правовые базы, содержащие программы, документы, аналитическую информацию;

2) базы «Справочники и программы по правовой тематике»;

3) электронный архив;

4) библиотека «Гарант» на бумажных носителях, информация из которой может передаваться пользователю в печатном виде.

Всего в базах хранится более 60 тыс. нормативных документов по следующим темам:

1) законодательство Российской Федерации (на русском языке);

2) законодательство Российской Федерации (на английском языке);

3) таможенное законодательство;

4) банковское законодательство;

5) землепользование, пользование недрами, охрана природы;

6) жилищное законодательство;

7) международное право;

8) налоговое право и бухгалтерский учет;

9) суд и арбитраж;

10) бухгалтерия;

11) формы правовых документов.

Компьютерная программа ГАРАНТ — это справочная правовая система, позволяющая работать с правовыми документами. Система разрабатывается с 1990г. В настоящее время она является основным инструментом принятия решения по правовым вопросам для многих бухгалтеров, юристов, руководителей, других специалистов в России и за рубежом. Полный объем информационного банка системы ГАРАНТ составляет более миллиона документов и комментариев к нормативным актам, причем еженедельное пополнение составляет около 4000 единиц документов. Информационный банк данных системы «Гарант» построен по модульному принципу и включает в себя 27 специализированных правовых блоков по всем разделам федерального законодательства и 132 правовых блока по законодательству субъектов Федерации. В системе ГАРАНТ представлено законодательство 73 регионов Российской Федерации, а также практика 10 Федеральных Арбитражных Судов. Пользователь сам выбирает наполнение базы данных, что позволяет использовать в работе документы, касающиеся именно его сферы деятельности. Система обладает современным, удобным интерфейсом, обеспечивающим максимальный комфорт и простоту в работе. Гибкая система персональных настроек позволяет специалисту получить результат, максимально учитывающий его индивидуальные потребности и опыт.

Все документы в системе ГАРАНТ представлены с комментариями и разъяснениями специалистов, в том числе там можно найти материалы из популярной бухгалтерской прессы.

В системе реализована уникальная технология поиска через Энциклопедию ситуаций. Пользователь формулирует запрос, используя привычные для него термины, а система в течение нескольких минут предоставляет ему ответ. Возможности, предоставляемые системой Гарант.

В системе представлены объединенные в одной программе все типы правовой информации — федеральное и региональное законодательство, международные договоры, комментарии, проекты законов, судебная и арбитражная практика, а также бизнес-справки, налоговый календарь, формы бухгалтерской и статистической отчетности, таблицы и схемы по вопросам законодательства и многое другое.

Проводится многоэтапная юридическая обработка документов в виде комментариев и ссылок на цитируемые нормативные акты, которая исключает неоднозначную трактовку материала, делает его актуальным и более понятным.

Поиск нужной информации осуществляется по всему информационному банку системы и позволяет получить не только документы федерального и регионального уровня, но и аналитические материалы, охватывающие данную проблему.

Формирование индивидуального информационно-правового комплекта для каждого пользователя. Разработаны специальные предложения для бухгалтеров, юристов, руководителей, а также строительных, фармацевтических и медицинских организаций.

Благодаря новой функции «Машина времени», пользователи системы ГАРАНТ Платформа F1 имеют уникальную возможность поиска текстов документов, действовавших в тот или иной момент времени. Функция «Постановка документов на контроль» автоматически отслеживает и предупреждает пользователя об изменениях в важных для него документах. В Платформе F1 пользователь может сопровождать текст документа собственными комментариями, причем, в них можно проставлять гипертекстовые ссылки на другие документы информационного банка.

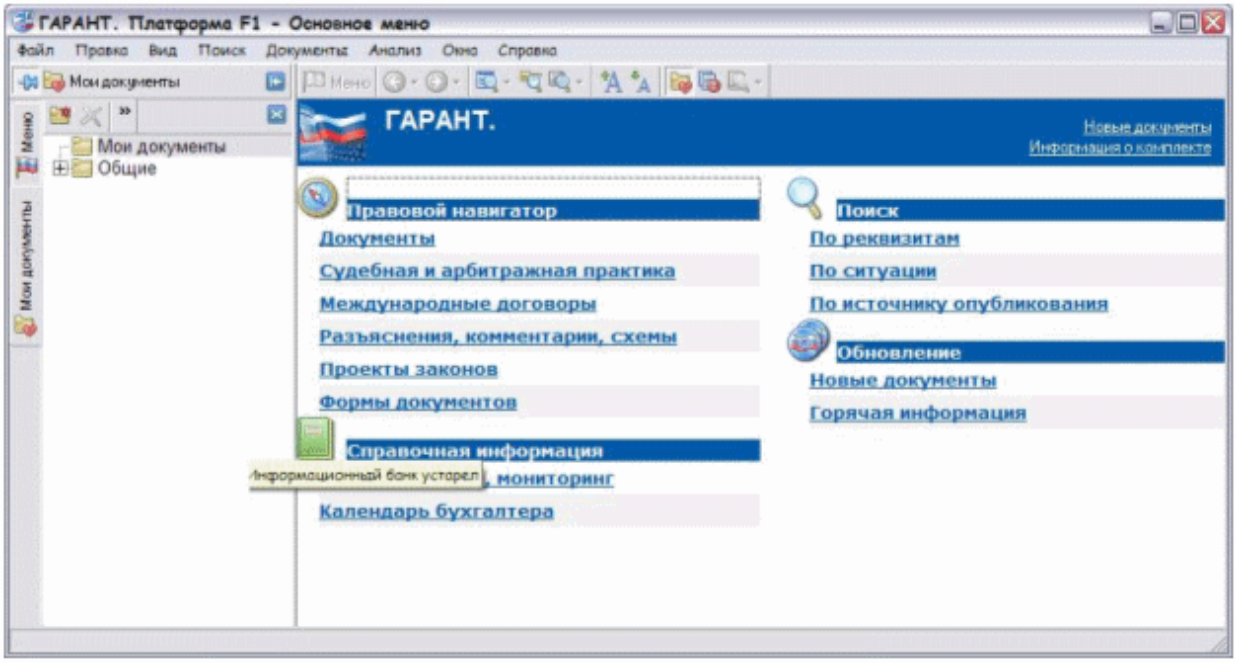
Объемные документы сопровождаются дополнительной информацией — структурой документа. Структура, реализованная в виде специальной вкладки, обеспечивает удобство в работе, позволяя одновременно расположить на экране содержание документа и его текст. В структуре приведено оглавление документа (главы, разделы и статьи),

а также ссылки на внедренные в текст графические объекты, шаблоны форм в формате MS Word и MS Excel, сохраненные пользователем персональные комментарии и закладки.

Система обладает рядом других новшеств, такими как «Графика в документе», «Контекстные фильтры», «История работы», «Примечания к папкам и закладкам», «Обмен результатами», упрощающих работу с правовой информацией и экономящих время.

Основное меню

Работа с системой ГАРАНТ Платформа F1 начинается с Основного меню (рис. 9.1) , с помощью которого вызываются все ключевые функции программы.



Основное меню позволяет переходить к следующим разделам:

Правовой навигатор;

Поиск по ситуации;

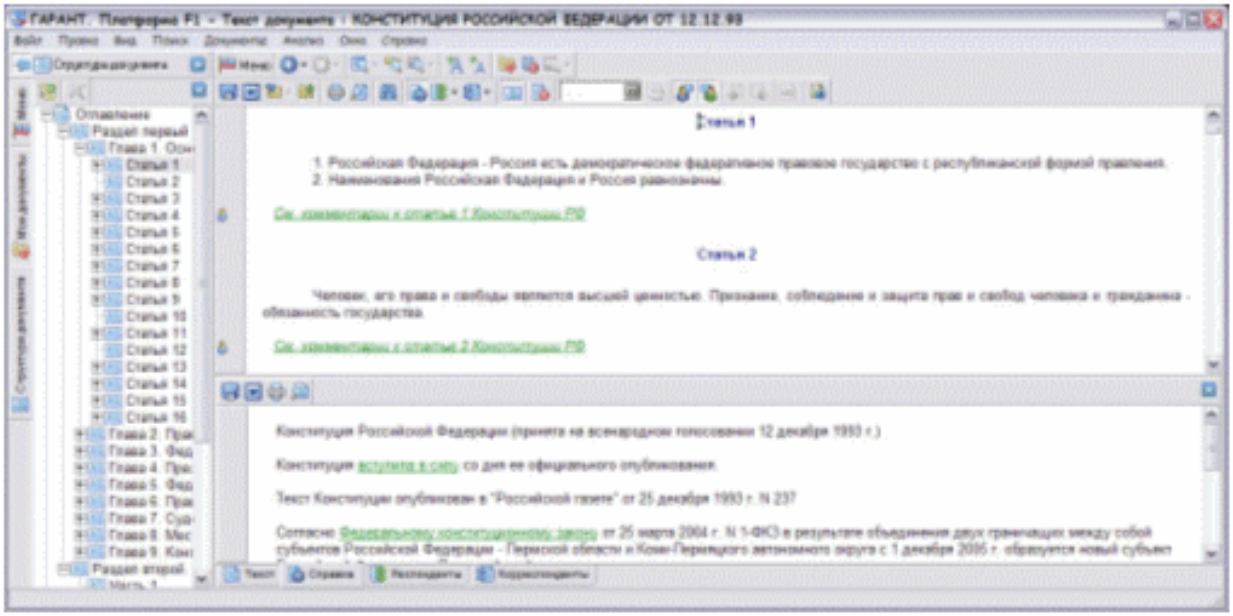
Поиск по реквизитам;

Справочная информация.

В любой момент работы с СПС «Гарант» можно перейти к основному меню, нажав на кнопку «Меню» на панели инструментов или кнопку F2 на клавиатуре. Для навигации между выполняемыми действиями используются кнопки «Вперед» и «Назад».

Главное окно системы

Композиция главного окна системы ГАРАНТ типична для современных Windows-приложений. Окно содержит главное меню, панель инструментов, панель навигации и дополнительное окно, которые окружают основное окно (рис. 9.2).



Основное окно системы — это основная рабочая область, в которой отображается текущий объект. Например, в нем могут размещаться классификатор информации, карточка поиска, список найденных документов, текст документа и т.п. При запуске системы в этом окне отображается основное меню.

Если с текущим объектом основного окна связана определенная информация, она размещается в дополнительном окне, которое расположено под основным окном. Доступ к данной информации осуществляется с помощью вкладок, расположенных в нижней части экрана. Набор доступных вкладок зависит от типа текущего объекта. Для документа и списка наборы вкладок отличаются. Например, для документа можно вызвать справку, списки его респондентов/корреспондентов, текст юридического предупреждения (если оно есть).

Панель навигации прикреплена к левой части главного окна и предназначена для быстрого и удобного перемещения между

определенными объектами и разделами системы. Переходы осуществляются с помощью вкладок, размещенных вертикально на боковой стороне панели. Набор вкладок панели навигации зависит от содержания основного окна. Например, вкладка фильтров показывается при работе со списком документов, вкладка с оглавлением документа актуальна только во время просмотра текста документа, а вкладка с редакциями документа появляется, если в данный документ вносились изменения.

В главном меню представлены следующие разделы: «Файл», «Правка», «Вид», «Поиск», «Документ», «Анализ», «Окна» и «Справка», в которых сгруппированы все операции, доступные программе. Каждый раздел объединяет несколько операций, назначение которых определено названием раздела.

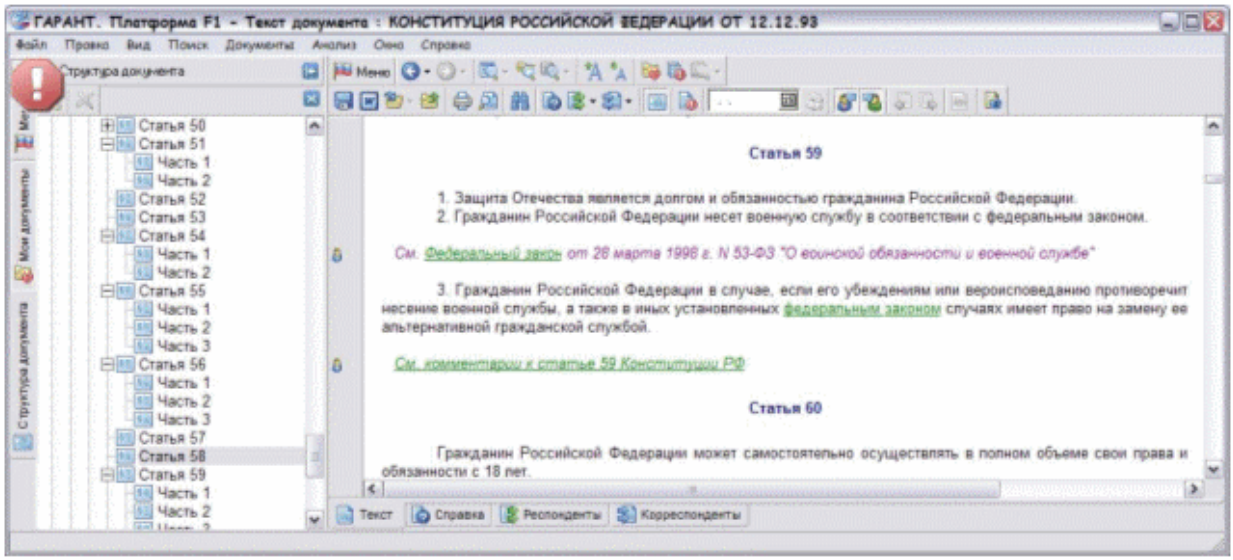
Наиболее часто используемые операции главного меню для удобства продублированы в системе кнопками панели инструментов. Состав панели инструментов меняется в зависимости от текущего рабочего объекта основного окна. Кроме того, состав и способ отображения кнопок панели инструментов могут быть настроены пользователем самостоятельно.

Документ

Документ системы ГАРАНТ представляет собой юридически обработанный текст исходного документа, снабженный исчерпывающей справочной информацией. Каждый документ, подключаемый к информационным ресурсам системы, проходит полный цикл юридической обработки, в результате которой работа с текстом документа становится удобнее и эффективнее. Благодаря удобной форме представления документов, предусматривающей особое цветовое оформление текста, гипертекстовые связи со всем массивом законодательства, встроенную графику и другие возможности, можно легко ориентироваться в сложной правовой информации.

Цветовое оформление текста

Для наглядности отдельные элементы текста документа выделены определенным цветом. На рис. 9.3 показано принятое оформление текстовых элементов документа.



Основной текст — обычный шрифт.

Так оформляются названия и заголовки.

Это гипертекстовая ссылка.

Так выглядит комментарий ГАРАНТа.

Таким шрифтом выделяются комментарии, которые вы можете добавлять в текст документа.

В системе ГАРАНТ реализовано единое гипертекстовое пространство. Все документы из любых информационных блоков ГАРАНТа связаны друг с другом гипертекстовыми ссылками. Каждое упоминание документа, входящего в состав системы, является ссылкой, которая по умолчанию выделяется в тексте зеленым цветом и подчеркивающей линией. При наведении курсора на гиперссылку всплывает подсказка, где сообщается название документа-респондента, на который она указывает.

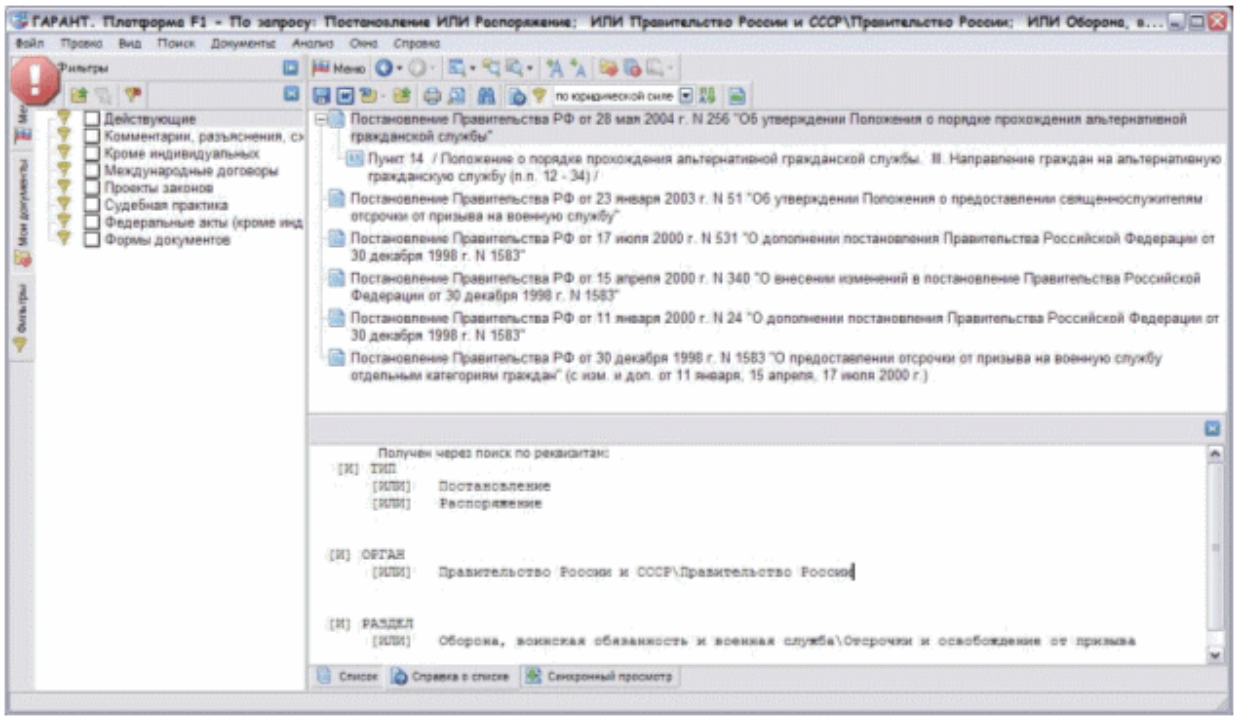
В процессе создания системы разработчиками устанавливается значительное число комментариев внутри документов. Комментарии добавляются, например, при внесении в документ официальных изменений, при выявлении в документе противоречий положениям нормативного акта большей юридической силы, несовпадении опубликованных в разных официальных источниках текстов одного документа, наличии других документов, регулирующих данный вопрос,

и. т.д. Комментарии юристов «Гаранта» по умолчанию выделяются сиреневым цветом и курсивом. При необходимости их можно скрыть с помощью кнопки  на панели инструментов. В системе также предусмотрена возможность добавлять в тексты документов собственные комментарии.

Оглавление документа отражает иерархию глав, пунктов, статей и других структурных единиц документа и отображается во вкладке «Структура документа» панели навигации. Курсор-указатель в оглавлении синхронизирован с видимой позицией в тексте документа. Выделение элемента оглавления приводит к переходу на соответствующий фрагмент в тексте документа. И, наоборот, прокрутка текста отражается на положении курсора в оглавлении. Одновременное расположение на экране текста документа и его оглавления удобно тем, что позволяет видеть, в какой части документа находится сейчас пользователь и дает возможность быстро перейти к любому другому фрагменту.

Список документов

Список появляется в результате поиска или навигации по правовому навигатору системы. Элементы списка являются ссылками на документы, при открытии которых система загружает требуемый документ (рис. 9.4).



На вкладке «Справка о списке», размещенной внизу списка, в дополнительном окне можно увидеть сведения о способе получения данного списка и последующих действиях, которые над ним были выполнены. Эти сведения помогут установить происхождение списка, например, при возврате к нему кнопкой «Назад».

При построении списка часто оказывается, что заданной теме удовлетворяет не документ целиком, а один или несколько конкретных его разделов: пункты, главы, статьи и другие структурные единицы документа. В таких случаях документы отображаются в списке не одной, а несколькими ссылками.

Поэтому списки документов в системе ГАРАНТ имеют вложенную, иерархическую структуру. Ссылки на найденные разделы документа «вкладываются» в название этого документа.

Документы в списке отображаются по-разному, в зависимости от того, подходит документ под заданную тему целиком или ей удовлетворяют только избранные разделы документа.

Документ подошел целиком. В списке приводится название документа. Переход в документе всегда выполняется на начало документа.

Найден один или несколько конкретных разделов. В списке приводится название документа, перед которым стоит значок «+». Под названием сгруппированы названия разделов. Ссылки на разделы имеют другой значок, отличный от значка документа. Переход по названию документа выполняется на начало первого вложенного раздела. Переход по названию вложенного раздела выполняется на начало данного раздела.

Поиск

Так как в базе данных СПС «Гарант» содержатся сотни тысяч правовых документов, для облегчения поиска нужных документов в ней реализованы мощнейшие механизмы поиска.

Основными системами поиска являются:

Правовой навигатор;

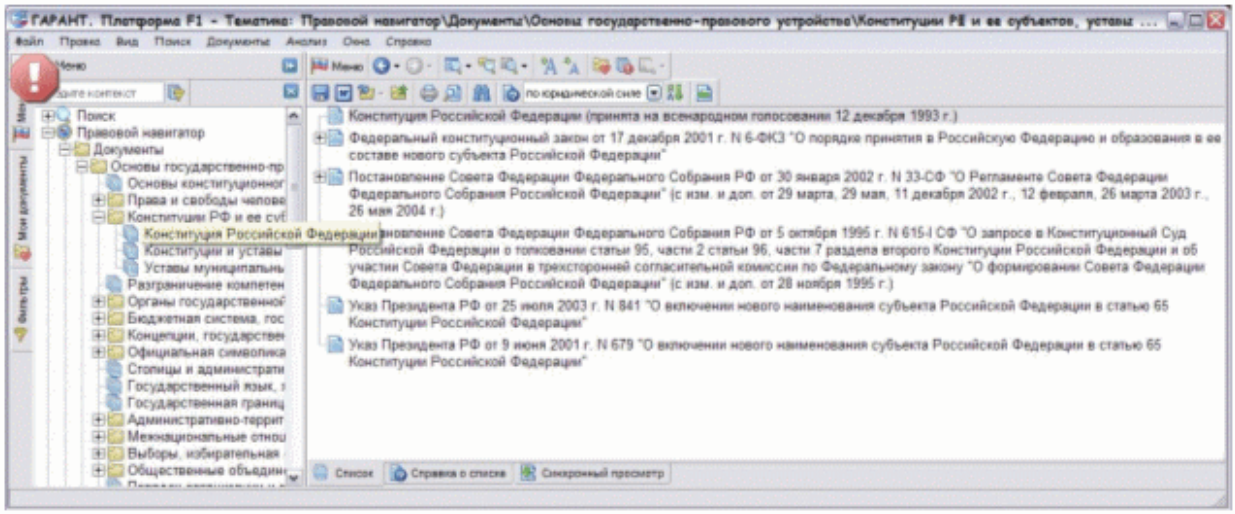
Поиск по ситуации;

Поиск по реквизитам.

Перейти к любому виду поиска можно из главного меню.

Поиск по разделам правового навигатора

Правовой навигатор в системе ГАРАНТ. Платформа F1 — это особый вид поиска по сочетанию двух типов классификаторов — тематического классификатора и классификатора видов правовой информации. Поиск по «Правовому навигатору» (рис. 9.5),



по сути, является поиском документа по тематическому оглавлению. Сначала следует определиться, правовую информацию

какого вида необходимо найти — правовые акты, судебную практику, международные договоры и т.д., и нажать на соответствующую надпись раздела «Правовой навигатор» главного меню, а затем последовательно уточнить запрос с помощью тематического классификатора, расположенного в основном окне, постепенно сужая круг рассматриваемых правовых тем.

На панели навигации показывается дерево папок, а в основное окно загружается содержимое выделенной папки. Окна синхронизируются друг с другом так, что переходы в одном из них автоматически выполняются и в другом. Можно видеть и сам рубрикатор, и список документов, найденных путем перехода к соответствующему разделу.

Классификация осуществляется по нормам права. В полученном списке документов при входе в текст объемных документов они открываются именно на тех фрагментах, которые отвечают по смыслу тематике выбранного подуровня. Для нормативных правовых документов — это конкретная норма права. Кроме того, многие нормы права могут быть отнесены к нескольким разделам рубрикатора, поэтому один и тот же документ можно найти в разных разделах.

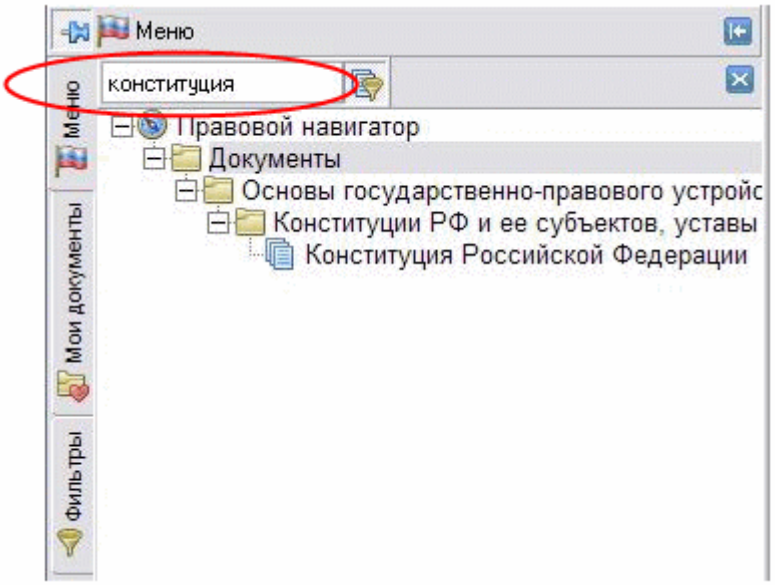
Поиск того или иного раздела в «Правовом навигаторе» можно осуществлять с помощью контекстного фильтра. Для этого достаточно набрать в произвольной последовательности в поле контекстного фильтра слова из названия раздела нужной тематики. В результате фильтрации в «Правовом навигаторе» останутся только те разделы, в которых их собственные наименования или наименования их подразделов соответствуют набранному контексту.

Поиск набранного контекста происходит тогда, когда кнопка «Включить контекстный фильтр» нажата.

Например, для того, чтобы найти текст Конституции Российской Федерации, нужно из панели навигации выбрать пункт «Документы» и раскрыть его, нажав на плюсик рядом с ним. Далее пункт «Основы государственно-правового устройства», в нем выбрать пункт «Конституция РФ и ее субъектов, уставы муниципальных образований» и

далее выделить пункт с названием «Конституция Российской Федерации». После чего в основном окне появится список документов, которые относятся к выбранному пункту. Среди них будет документ с названием «Конституция Российской Федерации», это и есть искомый документ. Для того, чтобы ознакомиться с его содержанием, нужно один раз нажать мышкой на его название в основном окне.

Можно найти данный документ быстрее, набрав в окне контекстного фильтра слово «конституция» (рис. 9.6).



Тогда в правовом навигаторе автоматически будут отобраны пункты, содержащие слово «конституция» в названии.

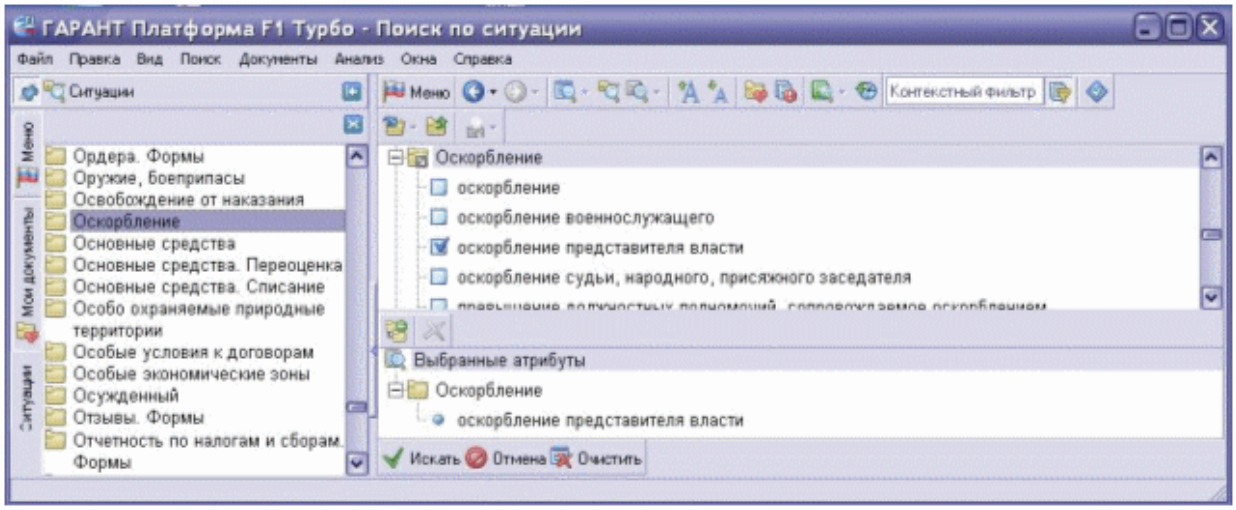
Поиск по ситуации

Поиск по ситуации целесообразно использовать в том случае, когда необходимо найти ответ на какой-либо правовой вопрос или узнать, какими правовыми документами регулируется та или иная ситуация, при этом какая-либо информация об искомом документе отсутствует.

Поиск по ситуации заключается в выборе из обширной энциклопедии ситуаций краткого, в одном предложении, описания практического вопроса. В ответ система выводит список документов, посвященных указанной тематике. Ссылки из этого списка направляют

пользователя непосредственно к тем фрагментам текста, которые посвящены заданной теме.

Чтобы выполнить поиск по ситуации, нужно нажать клавишу F5, кнопку панели инструментов «Поиск по ситуации» или выбрать пункт «Поиск по ситуации» главного меню (рис. 9.7). Система загрузит энциклопедию ситуаций.

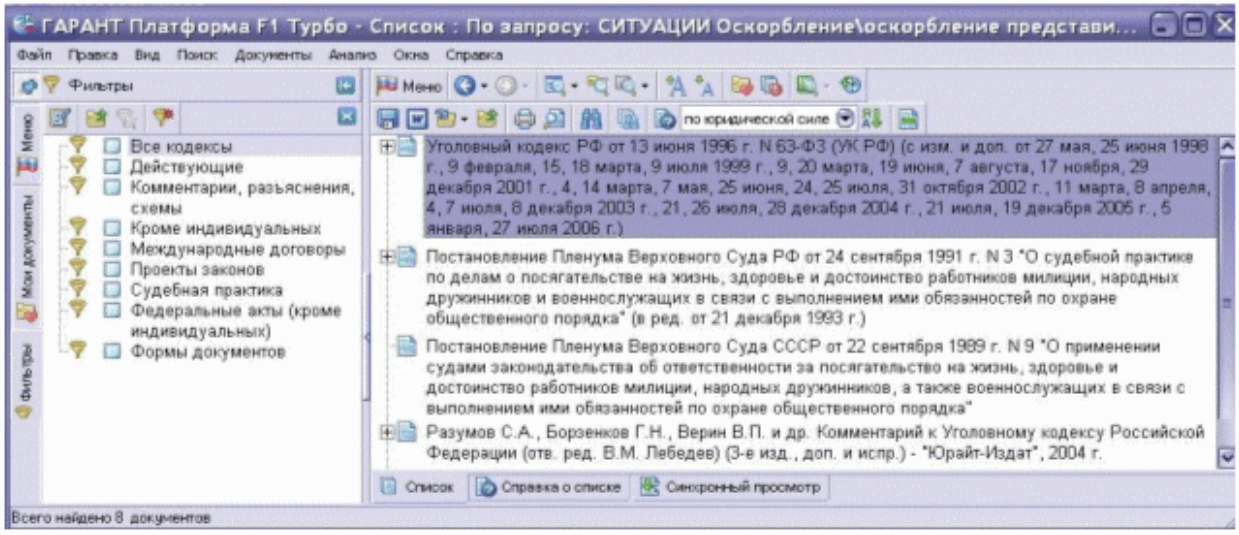


Описания ситуаций, или термины, представляют собой лаконичные формулировки конкретных правовых тем. Описания имеют два уровня — основной, который отображается на панели навигации, и дополнительный, отображаемый в основном окне. Описания основного уровня выражают относительно широкие понятия. При выделении пункта основного уровня он уточняется подчиненными ему описаниями дополнительного уровня в основном окне.

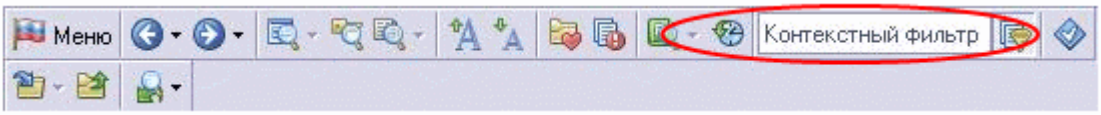
Например, для того, чтобы выяснить, какое наказание предусмотрено российским законодательством за оскорбление представителя власти, нужно в основном меню выбрать пункт «Оскорбление», после чего в дополнительном окне выбрать пункт «Оскорбление представителя власти». Потом поставить галочку в квадрат рядом с выбранным пунктом и нажать кнопку «Искать». При этом выбранный Вами пункт будет отображен в дополнительном окне.

В результате будет сформирован список правовых документов, которыми регулируется данная ситуация. Выбрав нужный документ, нужно один раз кликнуть на него мышкой, после чего он откроется для

просмотра именно в том месте, которое соответствует выбранной ситуации (рис. 9.8).



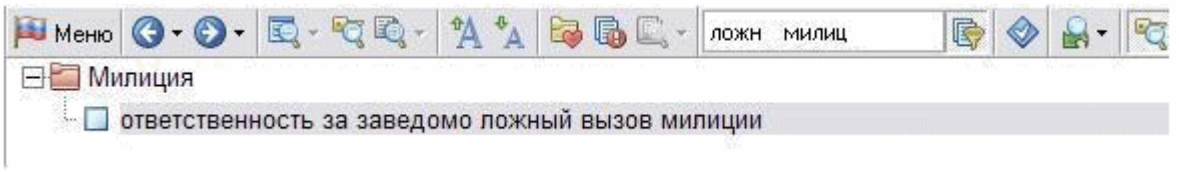
При поиске можно отмечать термины как основного, так и дополнительного уровней. Для ускорения поиска рекомендуется применять контекстный фильтр. Он расположен над основным окном во время выбора ситуации (рис. 9.9).



Если ввести в поле контекстного фильтра слово, то в основном окне будут отображены только те ситуации, которые содержат в названии данное слово. При этом все элементы списка, названия которых не содержат заданного слова, будут скрыты. Необязательно, чтобы искомое название начиналось с заданного слова. Оно может присутствовать и в середине названия, и в середине любого слова из названия. Можно ввести несколько слов — будут отобраны элементы, в которых присутствуют заданные слова в любом порядке. Редактирование строки контекста при включенном фильтре учитывается системой автоматически. По мере ввода или удаления символов выполняется повторная фильтрация списка. Следует учесть, что контекстный фильтр учитывает форму вводимого слова, то есть если ввести в контекстный фильтр слово «преступление», то ситуация «совершение преступлений группой лиц» найдена не будет, потому что эти слова не совпадают в окончании. Для того, чтобы в качестве результата получить все

словоформы искомого слова, необходимо в контекстный фильтр вводить искомое слово без окончания — «преступлен».

Например, необходимо найти какое наказание повлечет ложный вызов милиции. Наверняка в искомой ситуации должны содержаться два слова – «ложный» и «милиция». Если ввести их без окончаний через пробел в контекстный фильтр «ложн милиц», то будет найдена искомая ситуация «ответственность за заведомо ложный вызов милиции» (рис. 9.10).



Документ, найденный по описанию из энциклопедии ситуаций, может не содержать в тексте конкретных слов из выбранного описания, но при этом по смыслу отвечать запрошенной теме.

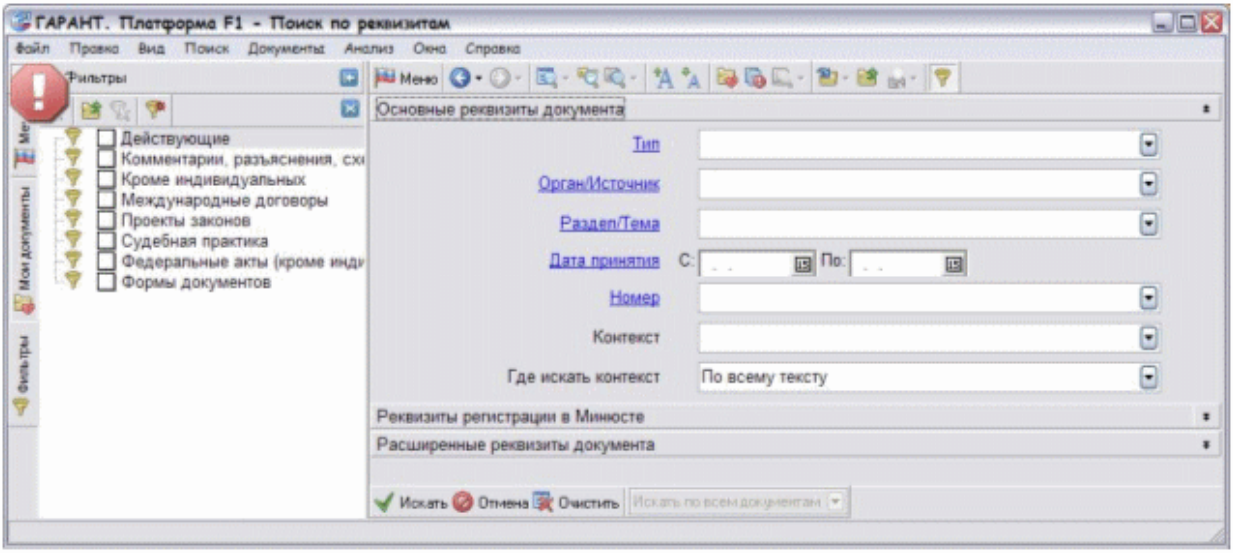
Обратите внимание, что некоторые описания синонимичны друг другу. Таким образом, одну и ту же проблему можно формулировать разными способами и получать при этом одинаковые результаты.

Как и при любом виде поиска, перед составлением нового запроса не забудьте очистить карточку запроса. Если оставить отмеченными лишние термины, то в результаты поиска попадет много ненужных документов.

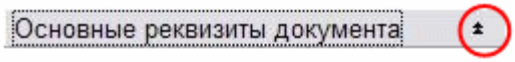
Поиск по реквизитам

Поиск по реквизитам предназначен для поиска документов по заранее известной или предполагаемой информации о документе. Он позволяет сочетать в запросе самую разнообразную информацию: тип и номер искомого документа, принявший орган и дату принятия, опубликования или регистрации в Минюсте, слова или словосочетания, содержащиеся в тексте документа, и многие другие реквизиты.

Для того, чтобы выполнить поиск документов по реквизитам, нужно нажать клавишу F7 или кнопку панели инструментов «Поиск по реквизитам» (рис. 9.11). После этого система загрузит карточку запроса.



Карточка запроса состоит из набора полей для ввода условий поиска. Условием является любое заполненное поле карточки, а их совокупность составляет поисковый запрос. В результате выполнения запроса выводится список документов, которые удовлетворяют всем введенным условиям одновременно. Поля карточки запроса разделены на секции: основные реквизиты и расширенные реквизиты. С целью экономии экранного пространства неиспользуемые секции можно сворачивать с помощью кнопки, расположенной справа от названия секции (рис. 9.12).



Карточка запроса состоит из следующих поисковых реквизитов.

«Тип»: тип искомого документа (закон, постановление). Чаще всего документ характеризуется единственным типом, который вытекает из названия самого документа.

«Орган/Источник»: название законодательного органа, принявшего искомый нормативный акт. Название источника обычно явствует из названия документа.

«Раздел/Тема». В этом поле задается тематика искомого документа, то есть его положение в классификаторе правовой информации. Данный классификатор норм права применяется в правовом навигаторе системы.

Если условиям поиска будет удовлетворять не документ целиком, а отдельные его разделы, статьи, пункты, абзацы, то такой документ также войдет в результаты поиска.

Поля «Тип», «Орган/Источник» и «Раздел/Тема» — имеют иерархическую структуру и представляют собой древовидную структуру, значения которой сгруппированы в папки. Группирующие папки обозначаются символом

- (желтая папка) а значения реквизитов символом
- (синий кружочек). В папки вложены уточняющие значения, которые, в свою очередь, также могут иметь внутреннюю структуру. При выборе папки в качестве значения реквизита, в качестве условий поиска автоматически выбираются все значения из выбранной папки. Для реквизитов, имеющих иерархическую структуру, нужно внимательно следить за тем, в какую папку входит отмечаемое значение. В частности, при выборе типа документа не следует путать типы, вложенные в раздел «Формы документов», с типами, размещенными на верхнем уровне списка. Например, результат поиска по типу Приказ не будет совпадать с результатом поиска по типу «Форма документа/Приказ». Во втором случае будут найдены только те документы, которые содержат в тексте бланки (формы) приказов. Или, например, если в поле «Орган/Источник» ввести значение «Президент России», то в качестве подсказки будет выведена именно папка «Президент России и СССР» со всеми входящими в нее значениями. Для того, чтобы выделить только президента России, нужно раскрыть папку (нажать на знак плюс рядом с ней) и щелкнуть мышкой по конкретному значению реквизита.

Дата принятия. Дата принятия документа органом власти. Карточка запроса содержит два поля для ввода даты: дата С: и дата По:. Это позволяет задавать как точную дату принятия, так и отрезок времени, закрытый или открытый. В случае заполнения обоих полей одинаковой датой ищется документ, принятый именно в этот день. В случае заполнения обоих полей разными датами, ищется документ, принятый за

указанный отрезок времени. А в случае заполнения только одного поля (либо С: либо По:) интервал поиска становится открытым.

Значение даты вводится либо с клавиатуры в формате дд.мм.гггг, либо выбирается с помощью электронного календаря.

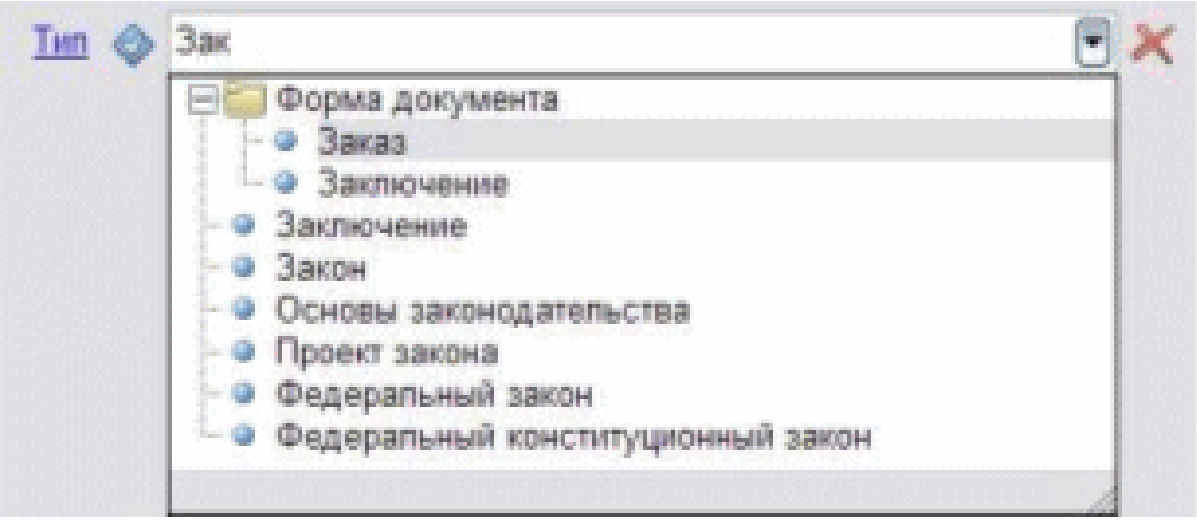
Номер. Номер искомого документа. Одному значению номера может соответствовать несколько документов, принятых в разное время разными органами. И, наоборот, совместно принятые документы могут иметь несколько номеров. Вместо окончания номера допускается ввод спецсимвола *, которым заменяется неизвестное окончание. Так, при использовании маски 221* будут найдены документы с номерами 221, 221-94, 221-П, 2216/98 и так далее.

Контекст. С помощью контекстного поиска можно найти документы, в текстах или в названиях которых содержатся определенные слова или словосочетания. При заполнении контекстного фильтра нужно быть уверенным в наличии искомого слова в документе. Если в тексте необходимо найти одно слово, то оно должно быть напечатано в поле контекст. Так как ИПС «Гарант» проводит поиск точного соответствия введенной и найденной формы слова, то для поиска всех форм слова необходимо писать его без окончания. Если в поле Контекст ввести словосочетание, то будет искаться заданная последовательность слов в тексте. Если требуется найти несколько слов в тексте документа, но при этом их взаимное расположение неизвестно, то искомые слова необходимо расположить в разных полях в пределах одного реквизита (как открыть несколько полей в пределах одного реквизита рассказывается ниже). Чтобы указать взаимное расположение двух слов в искомом документе, нужно воспользоваться полем «Где искать контекст».

Где искать контекст. Список выбора перечисляет возможные области поиска заданного контекста. Существует возможность проводить поиск заданного контекста: в названии документа, в пределах предложения, в пределах абзаца, либо по всему документу.

Условием поиска является любое заполненное поле карточки запроса. Значения реквизитов можно вводить непосредственно на

карточке запроса. Для этого нужно установить курсор в поле, соответствующее нужному реквизиту, и начать печатать искомое значение (рис. 9.13).



При этом система автоматически проследит за корректностью ввода. Вводимая строка по мере ввода будет сравниваться со значениями реквизита из базы данных, что послужит страховкой от любых ошибок. После начала ввода появится подсказка — выпадающий список выбора. Он будет содержать те значения реквизита, которые начинаются с набранных символов. Необязательно вводить нужную строку до конца. Чтобы выбрать значение из выпавшего списка, нужно переместить курсор стрелками клавиатуры и нажать Enter либо воспользоваться мышью. Выбранное значение будет подставлено в поле ввода.

После окончания формирования поискового запроса, для его выполнения нужно нажать на кнопку «Искать», расположенную внизу карточки поиска по реквизитам

. В зависимости от сложности запроса поиск занимает от долей секунды до нескольких минут. Особенно трудоемким является поиск с участием контекста. По окончании поиска система сообщит количество найденных документов и предложит вывести их список на экран.

В поисковый запрос можно включить произвольное количество условий для одного и того же реквизита (например, перечислить сразу

несколько возможных типов или эмитентов искомых документов). Для этой цели используется кнопка «Добавить», зеленый плюсик, расположенный справа от поля для ввода реквизита (рис. 9.14).

При нажатии кнопки появляется дополнительное поле ввода, расположенное напротив соответствующего реквизита. Кнопка добавления видна не всегда. Она появляется, когда для реквизита заполнено хотя бы одно поле. Кроме того, для некоторых реквизитов предусмотрено единственное поле ввода.

Кнопка «Удалить», красный крестик, расположенный справа от поля для ввода реквизита, очищает соответствующее условие поиска и удаляет поле ввода из карточки запроса. Если удаленное условие является для данного реквизита последним (единственным), то поле ввода очищается, но не удаляется.

Для некоторых реквизитов предусмотрено также логическое условие, с которым заданное значение будет участвовать в поиске. Значок логического условия размещается слева от поля ввода.

Эта кнопка-значок предназначена для индикации и переключения логического условия, с которым данное значение входит в поиск. Щелкая мышью по значку, можно циклически изменять условие между вариантами

— ИЛИ,

— И и

— КРОМЕ.

Логическое ИЛИ перед значением реквизита означает, что искомый документ должен обладать хотя бы одним значением из числа заданных

для данного реквизита с таким условием. Другими словами, при поиске будут отобраны документы, в свойствах которых имеются одно или несколько значений реквизита, заданных с условием ИЛИ.

Логическое И напротив значения реквизита означает, что искомый документ безусловно должен характеризоваться данным значением, причем независимо от выполнения других условий. Таким образом, документ будет удовлетворять всем таким условиям по отдельности.

Логическое КРОМЕ означает, что искомый документ не должен иметь заданное значение в числе своих свойств. Иначе говоря, из результатов поиска будут исключены все документы, обладающие таким значением. Ниже приводятся общие рекомендации по составлению поисковых запросов.

Очищайте карточку запроса. Команда «Очистить» удаляет все введенные условия поиска, то есть очищает все поля карточки запроса. Поисковый запрос становится пустым. Если запустить пустой запрос на исполнение, то система выведет список всех документов, содержащихся в текущем информационном банке. Если в карточке запроса одновременно присутствуют условия и нового, и предыдущего запросов, то результат поиска будет искажен. Поэтому рекомендуется очищать карточку всякий раз перед составлением нового поискового запроса.

Не задавайте слишком много условий. Как правило, для успешного поиска достаточно ввести условия для 2—3 реквизитов. Если результирующий список документов окажется слишком большим, то Вы сможете вернуться в карточку и уточнить запрос. Указать, например, номер и дату принятия обычно бывает достаточно для однозначной идентификации документа при поиске.

Вводите только точно известные значения. Не старайтесь заполнить карточку запроса всеми известными Вам реквизитами, особенно если есть сомнения в их достоверности. Ошибка хотя бы в одном условии приведет к тому, что нужный документ найден не будет. Поэтому старайтесь указывать только те условия, в которых Вы абсолютно уверены. В противном случае советуем применить «Поиск по ситуации» или воспользоваться «Правовым навигатором».

Оптимизируйте поиск контекста. Некоторые условия поиска контекста существенно увеличивают продолжительность поиска. Наличие любого из них требует дополнительного анализа документов, причем не всегда оправданного с точки зрения полноты и точности результатов. Перечислим эти условия.

Введено слово длиной более восьми символов. Совет: если нет явной необходимости, то вводите только первые восемь символов искомого слова. Система найдет все слова, которые начинаются с этих символов. Ситуации, когда требуется найти точную форму слова, встречаются исключительно редко. Напротив, задание слова в полной форме может привести к потере документов, в которых искомое слово имеет другие окончания.

Введено словосочетание. Используйте поиск словосочетания только для поиска устоявшихся последовательностей слов, в которых не может поменяться порядок слов, а также не могут быть вставлены дополнительные слова. Также поиск словосочетаний подходит для поиска документа, содержащего дословно известный Вам фрагмент или цитату. В остальных случаях для поиска близкорасположенных слов целесообразно применять поиск «в абзаце» или «в предложении».

Поиск в абзаце или предложении. Эти режимы поиска, описанные ниже, также увеличивают его продолжительность. Таким образом, наивысшая скорость поиска обеспечивается при поиске отдельных слов (не словосочетаний), каждое из которых задано в краткой форме. Так же быстро выполняется любой поиск контекста в названиях документов.

Поиск контекста в документе. Чтобы найти нужный фрагмент текста в пределах текущего документа применяется команда «Поиск контекста…». Она вызывает диалоговое окно «Поиск контекста». В этом поиске участвует весь видимый текст документа, включая все виды комментариев — при условии, что их отображение в момент поиска не выключено специальными командами.

9. Правовое обеспечение информационной безопасности

К правовым мерам обеспечения информационной безопасности относятся:

разработка норм, устанавливающих ответственность за компьютерные преступления;

защита авторских прав программистов;

совершенствование уголовного и гражданского законодательства;

совершенствование судопроизводства;

общественный контроль разработчиков компьютерных систем;

принятие соответствующих международных соглашений.

До недавнего времени в Российской Федерации отсутствовала возможность эффективной борьбы с компьютерными преступлениями, так как данные преступления не могли считаться противозаконными, поскольку они не квалифицировались уголовным законодательством. До 1 января 1997г. на уровне действующего законодательства России можно было считать удовлетворительно урегулированной лишь охрану авторских прав разработчиков программного обеспечения и, частично, защиту информации в рамках государственной тайны, но не были отражены права граждан на доступ к информации и защита информации, непосредственно связанные с компьютерными преступлениями.

Часть указанных пробелов была устранена после введения в действие с 1 января 1997г. нового Уголовного Кодекса, принятого Государственной Думой 24 мая 1996г. В новом УК ответственность за компьютерные преступления устанавливают ст.ст. 272, 273 и 274.

Ст. 272 нового УК устанавливает ответственность за неправомерный доступ к компьютерной информации (на машинном носителе в компьютере или сети компьютеров), если это привело к уничтожению, блокированию, модификации или копированию информации либо к нарушению работы вычислительной системы. Эта статья защищает право владельца на неприкосновенность информации в системе. Владельцем информационной системы может быть любое лицо, правомерно пользующееся услугами по обработке информации как

собственник вычислительной системы или как лицо, которое приобрело право ее использования. Преступное деяние, ответственность за которое предусмотрено ст. 272, состоит в неправомерном доступе к охраняемой законом компьютерной информации, который всегда имеет характер совершения определенных действий и может выражаться в проникновении в компьютерную систему путем использования специальных технических или программных средств, позволяющих преодолеть установленные системы защиты; незаконном применении действующих паролей или маскировке под законного пользователя для проникновения в компьютер, хищения носителей информации (при условии, что были приняты меры их охраны), если это повлекло уничтожение или блокирование информации. (Доступ считается правомерным, если он разрешен правообладателем, собственником информации или системы. Неправомерным является доступ, если лицо не имеет права доступа, либо имеет право на доступ, но осуществляет его с нарушением установленного порядка).

Для наступления уголовной ответственности обязательно должна существовать причинная связь между несанкционированным доступом к информации и наступлением предусмотренных ст. 272 последствий, тогда как случайное временное совпадение неправомерного доступа и сбоя в вычислительной системе, повлекшего указанные последствия, не влечет уголовной ответственности.

Неправомерный доступ к компьютерной информации должен осуществляться умышленно, т.е. совершая это преступление, лицо сознает, что неправомерно вторгается в компьютерную систему, предвидит возможность или неизбежность указанных в законе последствий, желает и сознательно допускает их наступление или относится к ним безразлично. Следовательно, с субъективной стороны преступление, предусмотренное ст. 272, характеризуется наличием прямого или косвенного умысла. Мотивы и цели данного преступления могут быть самыми разными: корыстными, направленными на причинение вреда (из хулиганских, конкурентных или иных побуждений) или проверку своих профессиональных способностей, и др.

Поскольку мотив и цель преступления формулировкой ст. 272 не учитываются, она может применяться к всевозможным компьютерным посягательствам.

Ст. 272 УК состоит из двух частей. В первой части наиболее серьезное наказание преступника состоит в лишении свободы сроком до двух лет. Часть вторая указывает в качестве признаков, усиливающих уголовную ответственность, совершение преступления группой лиц либо с использованием преступником своего служебного положения, а равно имеющим доступ к информационной системе, и допускает вынесение приговора сроком до пяти лет. При этом не имеет значения местонахождение объекта преступления (например, банка, к информации которого осуществлен неправомерный доступ в преступных целях), который может быть и зарубежным. По уголовному законодательству субъектами компьютерных преступлений могут быть лишь лица, достигшие 16-летнего возраста.

Ст. 272 УК не регулирует ситуации, когда неправомерный доступ к информации происходит по неосторожности, поскольку при расследовании обстоятельств доступа зачастую крайне трудно доказать преступный умысел. Так при переходах по ссылкам от одного компьютера к другому в сети Интернет, связывающей миллионы компьютеров, можно легко попасть в защищаемую информационную зону какого-либо компьютера, даже не замечая этого (хотя целью могут быть и преступные посягательства).

Ст. 273 УК предусматривает уголовную ответственность за создание, использование и распространение вредоносных программ для компьютеров или модификацию программного обеспечения, заведомо приводящее к несанкционированному уничтожению, блокированию, модификации, копированию информации либо к нарушению работы информационных систем. Статья защищает права владельца компьютерной системы на неприкосновенность хранящейся в ней информации. Вредоносными считаются любые программы, специально разработанные для нарушения нормального функционирования других компьютерных программ. Под нормальным функционированием

понимается выполнение операций, для которых эти программы предназначены, и которые определены в документации на программу. Наиболее распространенные вредоносные программы — компьютерные вирусы, логические бомбы, а также программы, известные как «троянский конь». Для привлечения к ответственности по ст. 273 необязательно наступление каких-либо нежелательных последствий для владельца информации, достаточен сам факт создания вредоносных программ или внесение изменений в уже существующие программы, заведомо приводящих к указанным в статье последствиям. Использованием программ считается их опубликование, воспроизведение, распространение и другие действия по введению в оборот. Использование программ может осуществляться путем записи в память компьютера или на материальный носитель, распространения по сетям либо путем иной передачи другим пользователям.

Уголовная ответственность по ст. 273 возникает уже в результате создания вредоносных программ, независимо от их фактического использования. Даже наличие исходных текстов программ является основанием для привлечения к ответственности. Исключение составляет деятельность организаций, разрабатывающих средства противодействия вредоносным программам и имеющих соответствующие лицензии. Статья состоит из двух частей, различающихся признаком отношения преступника к совершаемым действиям. Часть 1 предусматривает преступления, совершенные умышленно, с сознанием того, что создание, использование или распространение вредоносных программ заведомо должно привести к нарушению неприкосновенности информации. При этом ответственность наступает независимо от целей и мотивов посягательства, которые могут быть вполне позитивными (например, охрана личных прав граждан, борьба с техногенными опасностями, защита окружающей среды и т.п.). Максимальное наказание по первой части — лишение свободы сроком до трех лет. По части 2 дополнительный квалифицирующий признак — наступление тяжких последствий по неосторожности. В этом случае лицо сознает, что создает, использует или распространяет вредоносную программу или ее

носители и предвидит возможность наступления серьезных последствий, но без достаточных оснований рассчитывает их предотвратить, либо не предвидит этих последствий, хотя как высококвалифицированный программист могло и было обязано их предусмотреть. Поскольку последствия могут быть очень тяжкими (смерть или вред здоровью человека, опасность военной или иной катастрофы, транспортные происшествия), максимальное наказание по части 2 — семь лет лишения свободы.

Отметим, что в законе не говорится о степени нанесенного вреда в отличие от краж, когда различаются просто кража, кража в крупном размере и кража в особо крупном размере. Здесь устанавливается лишь факт преступления, а размер ущерба влияет лишь на оценку его тяжести и меру ответственности.

Наконец, ст. 274 УК устанавливает ответственность за нарушение правил эксплуатации компьютеров, компьютерных систем или сетей лицом, имеющим доступ к ним, повлекшее уничтожение, блокирование или модификацию охраняемой законом информации, если это деяние причинило существенный вред. Эта статья защищает интересы владельца компьютерной системы в отношении ее правильной эксплуатации и распространяется только на локальные вычислительные сети организаций. К глобальным вычислительным сетям, например к таким, как Интернет, эта статья неприменима. Под охраняемой законом информацией понимается информация, для которой в специальных законах установлен режим ее правовой защиты. Между фактом нарушения правил эксплуатации и наступившим существенным вредом должна быть обязательно установлена причинная связь и полностью доказано, что наступившие вредные последствия являются результатом именно нарушения правил. Оценку нанесенного вреда устанавливает суд исходя из обстоятельств дела, причем считается, что существенный вред менее значителен, чем тяжкие последствия.

Субъект этой статьи — лицо, в силу своих должностных обязанностей имеющее доступ к компьютерной системе и обязанное соблюдать установленные для них технические правила. Согласно части

1 этой статьи он должен совершать свои деяния умышленно; сознавать, что нарушает правила эксплуатации; предвидеть возможность или неизбежность неправомерного воздействия на информацию и причинение существенного вреда, желать или сознательно допускать причинение такого вреда или относиться к его наступлению безразлично. Наиболее строгое наказание в этом случае — лишение права занимать определенные должности или заниматься определенной деятельностью на срок до пяти лет, либо ограничение свободы на срок до двух лет. Ч. 2 ст. 274 предусматривает ответственность за те же деяния, не имевшие умысла, но повлекшие по неосторожности тяжкие последствия, например, за установку инфицированной программы без антивирусной проверки, что повлекло за собой серьезные последствия (крупный финансовый ущерб, транспортные происшествия, утрату важных архивов, нарушение работы системы жизнеобеспечения в больнице и др.). Мера наказания за это преступление устанавливается судом в зависимости от наступивших последствий, максимальное наказание — лишение свободы на срок до четырех лет.

Как видно, рассмотренные статьи УК не охватывают все виды компьютерных преступлений, разнообразие которых увеличивается вместе с прогрессом в области компьютерной техники и ее использованием. Кроме того, некоторые формулировки статей допускают неоднозначное истолкование, например в определении злостного умысла. Поэтому в дальнейшем возможно пополнение и усовершенствование этих статей.

10. Новое в законодательстве об информации и ИКТ

Принятый Государственной Думой 8 июля 2006г., одобренный Советом Федерации 14 июля 2006г. и опубликованный 29 июля 2006г. Федеральный закон от 27 июля 2006г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» направлен на регулирование отношений, возникающих при осуществлении права на поиск, получение, передачу, производство и распространение информации; применении информационных технологий; обеспечении защиты информации. Рассмотрим законодательство Российской Федерации об информации, информационных технологиях и о защите информации по состоянию на 1 сентября 2008 г. Надеемся, что это будет полезно будущим юристам и работникам органов государственной власти, связанным с информационно-коммуникационными технологиями.

Этот Федеральный закон (далее — Закон) («Собрание законодательства РФ», 31.07.2006, № 31 (ч. 1), ст. 3448) пришел на смену действовавшему до него закону со схожим названием — «Об информации, информатизации и защите информации» (от 20 февраля 1995г. № 24-ФЗ). (Собрание законодательства Российской Федерации, 1995, № 8, ст. 609.) Согласно Пояснительной записке, законопроект вносился на основании Плана действий по выработке мер, необходимых для ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных от 28 января 1981г.

Старый закон неоднократно критиковался за наличие пробелов, декларативность и бездейственность его норм. Но новый закон оказался еще лаконичней прежнего и не ввел никаких механизмов повышения его действенности. Он содержит 18 статей, причем последняя статья перечисляет положения, утратившие силу с введением этого закона.

Согласно ст. 1, закон регулирует отношения, возникающие при:

осуществлении права на поиск, получение, передачу, производство и распространение информации;

применении информационных технологий;

обеспечении защиты информации.

Положения Закона не распространяются на отношения, возникающие при правовой охране результатов интеллектуальной деятельности и приравненных к ним средств индивидуализации.

Ст. 2 Закона устанавливаются следующие основные понятия:

информация — сведения (сообщения, данные) независимо от формы их представления;

информационные технологии — процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов;

информационная система — совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств;

информационно-телекоммуникационная сеть — технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники;

обладатель информации — лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам;

доступ к информации — возможность получения информации и ее использования;

конфиденциальность информации — обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя;

предоставление информации — действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц;

распространение информации — действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц;

электронное сообщение — информация, переданная или полученная пользователем информационно-телекоммуникационной сети;

документированная информация — зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или в установленных законодательством Российской Федерации случаях ее материальный носитель;

оператор информационной системы — гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных.

В нем по-прежнему подтверждается конституционная свобода «поиска, получения, передачи, производства и распространения информации любым законным способом» (ст. 3), однако не предусмотрены реальные гарантии этой свободы.

Общество рассчитывало, что новый законопроект позволит устранить следующие противоречия:

1) имеющиеся пробелы и противоречия, в частности, приведение понятийного аппарата и механизмов регулирования в соответствие с практикой применения информационно-коммуникационных технологий, в том числе, определение понятий «информационная система», «информационно-телекоммуникационная сеть», «электронное сообщение» и др.;

2) модификация закрепленных в действующей редакции подходов к регулированию различных категорий информации;

3) необходимость решения актуальных проблем, которые обозначил опыт существования старого Федерального закона «Об информации, информатизации и защите информации» (например, определение правового статуса различных категорий информации, регулирование создания и эксплуатации информационных систем, установление общих требований к использованию информационно-телекоммуникационных сетей)

4) отсутствие необходимой правовой основы для реализации конституционных прав граждан, защиты общественных и государственных интересов в сфере использования современных информационно-коммуникационных технологий.

Что касается устранения имеющихся пробелов и создания необходимой правовой основы для реализации конституционных прав граждан, то, например, положения закона об оплате предоставляемой гражданам информации, вместо общего принципа бесплатности услуги по предоставлению гражданам содержащейся в органах власти информации, собранной на средства самих этих граждан (в виде налогов) — с определенными исключениями из него, устанавливают принцип платы за такую информацию с двумя исключениями. Одним из них стала такая норма как требование бесплатного доступа к сайтам органов государственной власти и органов местного самоуправления (пп. 1, п. 8, ст. 8).

В ст. 9 («Ограничения доступа к информации») закон ушел и от введения принципа, принятого в цивилизованных странах мира: ограничения должны быть четко установлены законом, быть необходимыми в демократическом обществе и пропорциональными целям защиты. Другими словами, ограничения права на доступ к информации должны быть оспоримыми, они могут быть признаны в установленном порядке недействующими в случае преобладания общественного интереса в разглашении информации

Решение актуальных проблем заключается, видимо, в норме п. 3 ст. 10, в соответствии с которой при использовании для распространения электронных писем лицо, распространяющее информацию, обязано обеспечить получателю информации возможность отказа от такой информации. Таким образом, мы все теперь сможем отказаться от Интернет-спама, отвечая на каждое рекламное предложение. Вот только насколько это средство будет эффективно?

Закон «благоразумно» переложил заботу о регламентации условий предоставления информации, предоставляемой в обязательном порядке, на Правительство Российской Федерации или соответствующие

государственные органы, то есть органы, заинтересованные в максимальной волоките (п. 4 ст. 14).

Новый закон подтвердил: профессиональная тайна, т.е. информация, полученная гражданами при исполнении ими профессиональных обязанностей или организациями при осуществлении ими определенных видов деятельности (профессиональная тайна), подлежит защите в случаях, если на эти лица федеральными законами возложены обязанности по соблюдению конфиденциальности такой информации (п. 5 ст. 9). Тем самым, с учетом положения ст. 41 Закона о СМИ, возникает еще одно основание считать видом такой тайны профессиональную тайну журналиста — со всеми вытекающими из этого последствиями.

Новый закон, как и прежний, продекларировал, что нарушение его требований влечет за собой дисциплинарную, гражданско-правовую, административную или уголовную ответственность в соответствии с законодательством Российской Федерации. Несмотря на продолжающуюся закрытость от граждан государственных ресурсов и тотальную открытость сведений о гражданах на «черном рынке» информации, нам неизвестно о случаях наступления такой ответственности по прежнему закону. Возникают сомнения в эффективности и «новых старых» норм. Одна из причин таких сомнений — отказ законодателя от принятой повсеместно в Европе и мире практики учреждения специального органа по контролю над соблюдением информационного законодательства, своего рода информационного прокурора с широкими полномочиями. Вот вам и учет требований европейских конвенций!

Наконец, загадкой остается признание утратившим силу Федерального закона от 4 июля 1996г. № 85-ФЗ «Об участии в международном информационном обмене» (Собрание законодательства Российской Федерации, 1996, № 28, ст. 3347). Этот закон был столь же декларативным, как и закон «Об информации, информатизации и защите информации», но он хотя бы закреплял те или иные полезные

принципы. При этом новый закон не касается сферы международного информационного обмена вовсе.

Согласно положениям Закона, правовое регулирование отношений, возникающих в сфере информации, информационных технологий и защиты информации, основывается на следующих принципах:

достоверность информации и своевременность ее предоставления;

недопустимость установления нормативными правовыми актами каких-либо преимуществ применения одних информационных технологий перед другими, если только обязательность применения определенных информационных технологий для создания и эксплуатации государственных информационных систем не установлена федеральными законами;

неприкосновенность частной жизни, недопустимость сбора, хранения, использования и распространения информации о частной жизни лица без его согласия;

обеспечение безопасности Российской Федерации при создании информационных систем, их эксплуатации и защите содержащейся в них информации;

открытость информации о деятельности государственных органов и органов местного самоуправления и свободный доступ к такой информации, кроме случаев, установленных федеральными законами;

равноправие языков народов Российской Федерации при создании информационных систем и их эксплуатации;

свобода поиска, получения, передачи, производства и распространения информации любым законным способом;

установление ограничений доступа к информации только федеральными законами.

Законодательство Российской Федерации об информации, информационных технологиях и о защите информации основывается на Конституции РФ, международных договорах Российской Федерации и состоит из настоящего Федерального закона и иных регулирующих отношения по использованию информации федеральных законов. Правовое регулирование отношений, связанных с организацией и

деятельностью средств массовой информации, осуществляется в соответствии с законодательством Российской Федерации о средствах массовой информации. Порядок хранения и использования включенной в состав архивных фондов документированной информации устанавливается законодательством об архивном деле в Российской Федерации.

Информация может являться объектом публичных, гражданских и иных правовых отношений. Закон устанавливает факт того, что информация может свободно использоваться любым лицом и передаваться одним лицом другому лицу, если федеральными законами не установлены ограничения доступа к информации либо иные требования к порядку ее предоставления или распространения. Информация в зависимости от категории доступа к ней подразделяется на общедоступную информацию, а также на информацию, доступ к которой ограничен федеральными законами (информация ограниченного доступа).

Информация, согласно п. 3 ст. 5 Закона, в зависимости от порядка ее предоставления или распространения подразделяется на:

информацию, свободно распространяемую;

информацию, предоставляемую по соглашению лиц, участвующих в соответствующих отношениях;

информацию, которая в соответствии с федеральными законами подлежит предоставлению или распространению;

информацию, распространение которой в Российской Федерации ограничивается или запрещается.

Обладателем информации может быть гражданин (физическое лицо), юридическое лицо, Российская Федерация, субъект Российской Федерации, муниципальное образование.

Обладатель информации, исходя из п. 4 ст. 7 Закона, если иное не предусмотрено иными федеральными законами, вправе:

разрешать или ограничивать доступ к информации, определять порядок и условия такого доступа;

использовать информацию, в том числе распространять ее, по своему усмотрению;

передавать информацию другим лицам по договору или на ином установленном законом основании;

защищать установленными законом способами свои права в случае незаконного получения информации или ее незаконного использования иными лицами;

осуществлять иные действия с информацией или разрешать осуществление таких действий.

Обладатель информации при осуществлении своих прав обязан:

соблюдать права и законные интересы иных лиц;

принимать меры по защите информации;

ограничивать доступ к информации, если такая обязанность установлена федеральными законами.

К общедоступной информации настоящим Законом относят общеизвестные сведения и иную информацию, доступ к которой не ограничен. Общедоступная информация может использоваться любыми лицами по их усмотрению при соблюдении установленных федеральными законами ограничений в отношении распространения такой информации. Обладатель информации, ставшей общедоступной по его решению, вправе требовать от лиц, распространяющих такую информацию, указывать себя в качестве источника такой информации.

Граждане и организации (юридические лица) (далее — организации) вправе осуществлять поиск и получение любой информации в любых формах и из любых источников при условии соблюдения требований, установленных настоящим Законом и другими федеральными законами. Гражданин имеет право на получение от государственных органов, органов местного самоуправления, их должностных лиц в порядке, установленном законодательством Российской Федерации, информации, непосредственно затрагивающей его права и свободы.

Организация имеет право на получение от государственных органов, органов местного самоуправления информации, непосредственно касающейся прав и обязанностей этой организации, а также информации, необходимой в связи с взаимодействием с указанными органами при осуществлении этой организацией своей уставной деятельности.

Не может быть ограничен доступ к:

нормативным правовым актам, затрагивающим права, свободы и обязанности человека и гражданина, а также устанавливающим правовое положение организаций и полномочия государственных органов, органов местного самоуправления;

информации о состоянии окружающей среды;

информации о деятельности государственных органов и органов местного самоуправления, а также об использовании бюджетных средств (за исключением сведений, составляющих государственную или служебную тайну);

информации, накапливаемой в открытых фондах библиотек, музеев и архивов, а также в государственных, муниципальных и иных информационных системах, созданных или предназначенных для обеспечения граждан (физических лиц) и организаций такой информацией;

иной информации, недопустимость ограничения доступа к которой установлена федеральными законами.

Государственные органы и органы местного самоуправления обязаны обеспечивать доступ к информации о своей деятельности на русском языке и государственном языке соответствующей республики в составе Российской Федерации в соответствии с федеральными законами, законами субъектов Российской Федерации и нормативными правовыми актами органов местного самоуправления. Лицо, желающее получить доступ к такой информации, не обязано обосновывать необходимость ее получения. Решения и действия (бездействие) государственных органов и органов местного самоуправления,

общественных объединений, должностных лиц, нарушающие право на доступ к информации, могут быть обжалованы в вышестоящий орган или вышестоящему должностному лицу либо в суд. В случае, если в результате неправомерного отказа в доступе к информации, несвоевременного ее предоставления, предоставления заведомо недостоверной или не соответствующей содержанию запроса информации были причинены убытки, такие убытки подлежат возмещению в соответствии с гражданским законодательством.

Предоставляется бесплатно информация:

о деятельности государственных органов и органов местного самоуправления, размещенная такими органами в информационно-телекоммуникационных сетях;

затрагивающая права и установленные законодательством Российской Федерации обязанности заинтересованного лица;

иная установленная законом информация.

Установление платы за предоставление государственным органом или органом местного самоуправления информации о своей деятельности возможно только в случаях и на условиях, которые установлены федеральными законами.

Ограничение доступа к информации устанавливается федеральными законами в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства. Обязательным является соблюдение конфиденциальности информации, доступ к которой ограничен соответствующими федеральными законами. Защита информации, составляющей государственную тайну, осуществляется в соответствии с законодательством Российской Федерации о государственной тайне.

Федеральные законы определяют условия отнесения информации к сведениям, составляющим коммерческую тайну, служебную тайну и иную тайну, обязательность соблюдения конфиденциальности такой информации, а также ответственность за ее разглашение.

Информация, полученная гражданами (физическими лицами) при исполнении ими профессиональных обязанностей или организациями при осуществлении ими определенных видов деятельности (профессиональная тайна), подлежит защите в случаях, если на эти лица федеральными законами возложены обязанности по соблюдению конфиденциальности такой информации. Информация, составляющая профессиональную тайну, может быть предоставлена третьим лицам только в соответствии с федеральными законами и (или) по решению суда.

Срок исполнения обязанностей по соблюдению конфиденциальности информации, составляющей профессиональную тайну, может быть ограничен только с согласия гражданина., предоставившего такую информацию о себе.

Запрещается требовать от гражданина предоставления информации о его частной жизни, в том числе информации, составляющей личную или семейную тайну, и получать такую информацию помимо воли гражданина, если иное не предусмотрено соответствующими федеральными законами.

Порядок доступа к персональным данным граждан устанавливается федеральным законом о персональных данных.

В Российской Федерации распространение информации осуществляется свободно при соблюдении требований, установленных законодательством Российской Федерации. Информация, распространяемая без использования средств массовой информации, должна включать в себя достоверные сведения о ее обладателе или об ином лице, распространяющем информацию, в форме и в объеме, которые достаточны для идентификации такого лица.

При использовании для распространения информации средств, позволяющих определять получателей информации, в том числе почтовых отправлений и электронных сообщений, лицо, распространяющее информацию, обязано обеспечить получателю информации возможность отказа от такой информации. Предоставление

информации осуществляется в порядке, который устанавливается соглашением лиц, участвующих в обмене информацией.

Случаи и условия обязательного распространения информации или предоставления информации, в том числе предоставление обязательных экземпляров документов, устанавливаются соответствующими федеральными законами. Запрещается распространение информации, которая направлена на пропаганду войны, разжигание национальной, расовой или религиозной ненависти и вражды, а также иной информации, за распространение которой предусмотрена уголовная или административная ответственность.

В федеральных органах исполнительной власти документирование информации осуществляется в порядке, устанавливаемом Правительством Российской Федерации. Правила делопроизводства и документооборота, установленные иными государственными органами, органами местного самоуправления в пределах их компетенции, должны соответствовать требованиям, установленным Правительством Российской Федерации в части делопроизводства и документооборота для федеральных органов исполнительной власти.

Электронное сообщение, подписанное электронной цифровой подписью или иным аналогом собственноручной подписи, признается электронным документом, равнозначным документу, подписанному собственноручной подписью, в случаях, если соответствующими федеральными законами или иными нормативными правовыми актами не устанавливается или не подразумевается требование о составлении такого документа на бумажном носителе.

В целях заключения гражданско-правовых договоров или оформления иных правоотношений, в которых участвуют лица, обменивающиеся электронными сообщениями, обмен электронными сообщениями, каждое из которых подписано электронной цифровой подписью или иным аналогом собственноручной подписи отправителя такого сообщения, в порядке, установленном федеральными законами, иными нормативными правовыми актами или соглашением сторон, рассматривается как обмен документами. Право собственности и иные

вещные права на материальные носители, содержащие документированную информацию, устанавливаются гражданским законодательством.

Согласно ст. 12 Закона государственное регулирование в сфере применения информационных технологий предусматривает:

регулирование отношений, связанных с поиском, получением, передачей, производством и распространением информации с применением информационных технологий (информатизации), на основании принципов, установленных настоящим Федеральным законом;

развитие информационных систем различного назначения для обеспечения граждан (физических лиц), организаций, государственных органов и органов местного самоуправления информацией, а также обеспечение взаимодействия таких систем;

создание условий для эффективного использования в Российской Федерации информационно-телекоммуникационных сетей, в том числе сети Интернет и иных подобных информационно-телекоммуникационных сетей.

Государственные органы, органы местного самоуправления в соответствии со своими полномочиями:

участвуют в разработке и реализации целевых программ применения информационных технологий;

создают информационные системы и обеспечивают доступ к содержащейся в них информации на русском языке и государственном языке соответствующей республики в составе Российской Федерации.

Ст. 13 Закона оговаривает понятие «Информационные системы». Согласно указанной статье понятие «Информационные системы» включают в себя:

государственные информационные системы — федеральные информационные системы и региональные информационные системы, созданные на основании соответственно федеральных законов, законов субъектов Российской Федерации, на основании правовых актов государственных органов;

муниципальные информационные системы, созданные на основании решения органа местного самоуправления;

иные информационные системы.

Если иное не установлено федеральными законами, оператором информационной системы является собственник используемых для обработки содержащейся в базах данных информации технических средств, который правомерно пользуется такими базами данных, или лицо, с которым этот собственник заключил договор об эксплуатации информационной системы. Права обладателя информации, содержащейся в базах данных информационной системы, подлежат охране независимо от авторских и иных прав на такие базы данных. Установленные настоящим Законом требования к государственным информационным системам распространяются на муниципальные информационные системы, если иное не предусмотрено законодательством Российской Федерации о местном самоуправлении. Особенности эксплуатации государственных информационных систем и муниципальных информационных систем могут устанавливаться в соответствии с техническими регламентами, нормативными правовыми актами государственных органов, нормативными правовыми актами органов местного самоуправления, принимающих решения о создании таких информационных систем.

Порядок создания и эксплуатации информационных систем, не являющихся государственными информационными системами или муниципальными информационными системами, определяется операторами таких информационных систем в соответствии с требованиями, установленными настоящим Федеральным законом или другими федеральными законами.

Государственные информационные системы создаются в целях реализации полномочий государственных органов и обеспечения обмена информацией между этими органами, а также в иных установленных федеральными законами целях. Государственные информационные системы создаются и эксплуатируются на основе статистической и иной документированной информации, предоставляемой гражданами

(физическими лицами), организациями, государственными органами, органами местного самоуправления.

Перечни видов информации, предоставляемой в обязательном порядке, устанавливаются федеральными законами, условия ее предоставления — Правительством Российской Федерации или соответствующими государственными органами, если иное не предусмотрено федеральными законами.

Правительство Российской Федерации вправе устанавливать обязательные требования к порядку ввода в эксплуатацию отдельных государственных информационных систем.

Не допускается эксплуатация государственной информационной системы без надлежащего оформления прав на использование ее компонентов, являющихся объектами интеллектуальной собственности.

Информация, содержащаяся в государственных информационных системах, а также иные имеющиеся в распоряжении государственных органов сведения и документы являются государственными информационными ресурсами.

На территории Российской Федерации использование информационно-телекоммуникационных сетей осуществляется с соблюдением требований законодательства РФ в области связи, настоящего Закона и иных нормативных правовых актов Российской Федерации.

Регулирование использования информационно-телекоммуникационных сетей, доступ к которым не ограничен определенным кругом лиц, осуществляется в Российской Федерации с учетом общепринятой международной практики деятельности саморегулируемых организаций в этой области. Порядок использования иных информационно-телекоммуникационных сетей определяется владельцами таких сетей с учетом требований, установленных настоящим Законом.

Соответствующими федеральными законами может быть предусмотрена обязательная идентификация личности, организаций, использующих информационно-телекоммуникационную сеть при

осуществлении предпринимательской деятельности. При этом получатель электронного сообщения, находящийся на территории РФ, вправе провести проверку, позволяющую установить отправителя электронного сообщения, а в установленных соответствующими федеральными законами или соглашением сторон случаях обязан провести такую проверку.

Передача информации посредством использования информационно-телекоммуникационных сетей осуществляется без ограничений при условии соблюдения установленных соответствующими федеральными законами требований к распространению информации и охране объектов интеллектуальной собственности. Передача информации может быть ограничена только в порядке и на условиях, которые установлены соответствующими федеральными законами.

Согласно ст. 16 Закона, защита информации представляет собой принятие правовых, организационных и технических мер, направленных на:

обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;

соблюдение конфиденциальности информации ограниченного доступа;

реализацию права на доступ к информации.

Обладатель информации, оператор информационной системы в случаях, установленных законодательством РФ, обязаны обеспечить:

предотвращение несанкционированного доступа к информации и (или) передачи ее лицам, не имеющим права на доступ к информации;

своевременное обнаружение фактов несанкционированного доступа к информации;

предупреждение возможности неблагоприятных последствий нарушения порядка доступа к информации;

недопущение воздействия на технические средства обработки информации, в результате которого нарушается их функционирование;

возможность незамедлительного восстановления информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней;

постоянный контроль за обеспечением уровня защищенности информации.

Требования о защите информации, содержащейся в государственных информационных системах, устанавливаются федеральным органом исполнительной власти в области обеспечения безопасности и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, в пределах их полномочий. При создании и эксплуатации государственных информационных систем, используемых в целях защиты информации, методы и способы ее защиты должны соответствовать указанным требованиям.

Нарушение требований настоящего Закона влечет за собой дисциплинарную, гражданско-правовую, административную или уголовную ответственность в соответствии с законодательством РФ. Лица, права и законные интересы которых были нарушены в связи с разглашением информации ограниченного доступа или иным неправомерным использованием такой информации, вправе обратиться в установленном порядке за судебной защитой своих прав, в том числе с исками о возмещении убытков, компенсации морального вреда, защите чести, достоинства и деловой репутации. Требование о возмещении убытков не может быть удовлетворено в случае предъявления его лицом, не принимавшим мер по соблюдению конфиденциальности информации или нарушившим установленные законодательством РФ требования о защите информации, если принятие этих мер и соблюдение таких требований являлись обязанностями данного лица.

Когда распространение определенной информации ограничивается или запрещается соответствующими федеральными законами, гражданско-правовую ответственность за распространение такой информации не несет лицо, оказывающее услуги:

по передаче информации, предоставленной другим лицом, при условии ее передачи без изменений и исправлений;

по хранению информации и обеспечению доступа к ней при условии, что это лицо не могло знать о незаконности распространения информации.