ВЫСШЕЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАНИЕ

ОРГАНИЗАЦИОННО-ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Под редакцией члена-корреспондента Академии криптографии Российской Федерации, профессора А. А. Стрельцова

Рекомендовано Учебно-методическим объединением по образованию в области информационной безопасности в качестве учебного пособия для студентов высших учебных заведений, обучающихся по специальностям 090102 «Компьютерная безопасность», 090105 «Комплексное обеспечение информационной безопасности автоматизированных систем», 090106 «Информационная безопасность телекоммуникационных систем»

ACADEMA

Москва
Издательский центр «Академия»
2008

УДК 65.012.45(075.8)
ББК 73я73
О-641

Авторы:
А.А. Стрельцов, В.С. Горбатов, Т.А. Полякова, Т.А. Кондратьева,
О.В. Дамаскин, Е.Б. Белов, С.Ю. Савин

Рецензенты:
д-р юр. наук, канд. техн. наук, проф. *А.В. Морозов*
(зав. кафедрой информационного права, информатики
и математики Российской правовой академии Министерства юстиции России);
д-р техн. наук, проф. *В.А. Конявский* (зав. кафедрой защиты информации
МФТИ)

Организационно-правовое обеспечение информационной
О-641безопасности : учеб. пособие для студ. высш. учеб. заведений /
А.А. Стрельцов [и др.] ; под ред. А.А. Стрельцова. — М. : Издательский центр «Академия», 2008. — 256 с.
ISBN 978-5-7695-4240-4

В пособии раскрыты положения, связанные со структурой правового обеспечения информационной безопасности и соответствующего законодательства в области информации, информационных технологий и защиты информации, персональных данных, интеллектуальной собственности, государственной тайны, электронной цифровой подписи, технического регулирования. Изложены вопросы юридической ответственности за правонарушения в области информационной безопасности, а также механизмы защиты прав и законных интересов субъектов информационной сферы. Значительное внимание уделено построению систем организационного обеспечения информационной безопасности.

Для студентов высших учебных заведений. Может быть полезно лицам, интересующимся проблематикой правового обеспечения информационной безопасности.

УДК 65.012.45(075.8)
ББК 73я73

ISBN 978-5-7695-4240-4

ПРЕДИСЛОВИЕ

Человечество вступило в новый этап развития, получивший название «информационное общество». На данном этапе важнейшим фактором экономического развития являются научные знания. Их внедрение на базе современных информационных технологий в средства производства позволяет добиваться существенного повышения производительности труда в промышленности, придает качественно новые потребительские свойства продукции промышленного производства и способствует повышению качества жизни человека.

Процесс создания таких знаний, их промышленного освоения и продвижения на рынке наукоемких товаров приобретает глобальный характер, привлекает все большие людские ресурсы, заметно изменяя социальную структуру общества, превращая информационные технологии в фактор общественного развития.

Одновременно объективное усиление зависимости общества от информационных технологий, глобальной информационной инфраструктуры, свободы трансграничного информационного обмена порождает угрозу использования этой зависимости во вред обществу. Расширяется область применения информационных технологий для совершения преступлений, нарушения устойчивости функционирования важных объектов инфраструктуры общества, подготовки и осуществления террористических актов и другой социально опасной деятельности.

Данные обстоятельства приводят к тому, что выявление угроз безопасности интересов личности, общества и государства в информационной сфере, предупреждение и пресечение их проявлений, а также ликвидация последствий проявления таких угроз рассматриваются в Российской Федерации в качестве важной составляющей обеспечения национальной безопасности.

Подготовка кадров по вопросам обеспечения информационной безопасности осуществляется по семи основ-

ным специальностям в более чем 100 высших учебных заведениях. В рамках этих специальностей изучается, в частности, организационно-правовое обеспечение информационной безопасности. В то же время количество учебников и учебных пособий по данному вопросу весьма незначительно.

Настоящее учебное пособие подготовлено в соответствии с курсом «Организационное и правовое обеспечение информационной безопасности», предусмотренным государственным образовательным стандартом высшего профессионального образования.

В пособии в систематизированном виде изложены наиболее важные вопросы правового и организационного обеспечения информационной безопасности. Структурно книга состоит из трех частей.

Первая часть «Основы теории обеспечения информационной безопасности» включает 4 главы, в которых раскрываются роль и место информационной безопасности в обеспечении устойчивого развития общества на новой, постиндустриальной стадии этого процесса, сущность информации как явления жизни человека и общества, содержание и формы обеспечения информационной безопасности как направления человеческой деятельности.

Вторая часть пособия «Правовое обеспечение информационной безопасности» состоит из 11 глав, посвященных вопросам правового обеспечения информационной безопасности, а также основным положениям законодательных актов, регулирующих отношения в рассматриваемой области.

Третья часть пособия «Организационное обеспечение информационной безопасности» включает 4 главы, в которых анализируются вопросы управления персоналом, организации объектовых режимов и некоторые другие аспекты организационного обеспечения информационной безопасности.

В подготовке материала учебного пособия принимал участие коллектив авторов. Так, гл. 1—4, 7—13 написаны д-ром техн. наук, д-ром юр. наук, проф. А. А. Стрельцовым, гл. 5 — А. А. Стрельцовым и доц. Т. А. Кондратьевой (5.1.), гл. 6 — А. А. Стрельцовым и канд. юр. наук, доц. Т. А. Поляковой (6.2), гл. 14 — д-ром юр. наук, проф. О. В. Дамаскиным, гл. 15 — С. Ю. Савиным, гл. 16—18 — канд. техн. наук, доц. В. С. Горбатовым, гл. 19 — В. С. Горбатовым и Е. Б. Беловым (19.3).

Считаю своим долгом выразить признательность директору Института проблем информационной безопас-

ности МГУ им. М. В. Ломоносова В. П. Шерстюку, генеральному директору компании «Элвис+» А. В. Соколову, начальнику Института криптографии, связи и информатики Академии ФСБ России А. П. Коваленко, директору Всероссийского научно-исследовательского института проблем вычислительной техники и информатизации В. А. Конявскому, заведующему кафедрой Московского высшего технического училища им. Н. Э. Баумана М. П. Сычеву за ценные замечания, которые позволили устранить недостатки пособия.

Трудно переоценить предложения проф. С. В. Коновченко по материалу книги, позволившие по-новому взглянуть на некоторые важные положения пособия и принятые авторским коллективом с благодарностью.

А. А. Стрельцов

ЧАСТЬ I
ОСНОВЫ ТЕОРИИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Глава 1
ИНФОРМАЦИОННОЕ ОБЩЕСТВО И ЕГО БЕЗОПАСНОСТЬ

1.1. Информационное общество — новый этап развития человечества

Информационное общество — новый этап развития человеческой цивилизации, характеризуемый прежде всего значительным повышением уровня использования во всех сферах жизнедеятельности общества накопленных человечеством знаний, достигаемым посредством активного применения современных информационных технологий, средств вычислительной техники, коммуникаций и связи.

В основе этого этапа развития лежит разрешение противоречия между огромным объемом знаний, накопленных человечеством за время его существования (особенно в рамках продолжающейся научно-технической революции), и ограниченными возможностями их использования в индустриальном обществе. Данное противоречие разрешается на базе использования современных информационных технологий и достижения высоких социальных стандартов жизни людей, предоставляющих достаточно возможностей для духовного развития и совершенствования.

Такое влияние информационных технологий, вычислительной техники, средств коммуникации и связи на общественное развитие объясняется в первую очередь их уникальными возможностями материализации результатов интеллектуальной деятельности человека в производственной деятельности, в том числе в области генерации новых знаний, возможностями распространения и потребления информации, освоения накопленных знаний членами общества. С помощью этих технологий могут быть существенно повышены глубина и качество обработки информации, используемой в средствах производства, обеспечения социальной коммуникации и общежития, в предметах потребления, в средствах ведения вооруженной борьбы. В результате возникает новое качество жизни общества, проявляющееся в экономической, социальной и духовной сферах, а также в сфере государственного управления.

Экономическая сфера определяется совокупностью отношений, складывающихся в процессе обеспечения общества средствами к существованию: пищей, одеждой, жильем, средствами коммуникации, другими предметами потребления, необходимыми членам общества и государству.

В составе экономической сферы выделяются производство, распределение и потребление. Производство охватывает отношения, связанные с созданием продуктов потребления и оказанием услуг в промышленности, сельском хозяйстве и других областях деятельности человека. Распределение охватывает отношения, связанные с доведением продуктов производства до потребителя, а потребление — отношения, связанные с использованием продуктов и услуг, необходимых для удовлетворения потребностей граждан и государства.

Развитие и использование современных информационных технологий, с одной стороны, привнесло много нового в традиционную экономику, изменяя соотношение между традиционными секторами экономической деятельности и «информационной» экономикой, с другой — способствовало возникновению новой формы реализации экономических отношений — «электронно-сетевой».

Отличительной чертой «информационной» экономики является сравнительно более высокая экономическая эффективность деятельности по развитию и реализации информационных технологий (по сравнению с деятельностью по производству товаров, обладающих натурально-вещественной формой) и энергии. Величина издержек производства все больше зависит от размеров нематериальных инвестиций — затрат на научные исследования и разработки, приобретение патентов и лицензий, образование и профессиональную подготовку кадров, программное обеспечение, инжиниринговые и консалтинговые услуги, маркетинг, рекламу, совершенствование структуры управления и т. п. В силу этого научные знания начинают непосредственно определять параметры экономического роста, создавая основу для инноваций и формирования квалифицированной рабочей силы. На долю наукоемких отраслей обрабатывающей промышленности и сферы услуг в настоящее время приходится в среднем более половины внутреннего валового продукта ведущих индустриальных стран. Данные отрасли отличаются наиболее высокими темпами роста объемов производства, занятости, инвестиций, внешнеторгового оборота. При этом достижения науки и техники являются ключевым фактором улучшения качества продукции и услуг, увеличения производительности труда, совершенствования организации производства. Все вышеперечисленное в конечном счете предопределяет конкурентоспособность предприятий и выпускаемой ими продукции на внутреннем и мировом рынках.

В силу того что информационные технологии образуют универсальный технологический базис всех видов производственной деятельности, возрастает значение секторов экономики, связанных с созданием средств ее интеллектуализации. Речь идет в первую очередь о научном приборостроении, производстве средств вычислительной техники и программного обеспечения. Параллельно развивается сектор услуг по обслуживанию вычислительной техники и процессов обработки информации, консультированию, научно-информационному обеспечению, выполнению информационно-вычислительных работ.

Особенность новой «электронно-сетевой» формы реализации экономических отношений заключается в многоуровневой пространственной структуре этих отношений и использовании для их поддержания составляющих глобальной информационной инфраструктуры, в том числе системы Интернет, информационных и коммуникационных сетей, сетей связи. В рамках данного сектора экономики развиваются индустрия новых информационных технологий и информационных продуктов, телекоммуникационные и провайдерские услуги, электронный бизнес, электронные рынки, электронные биржи, «телебанкинг», «телеработа» и другие виды экономической деятельности.

Современные информационные технологии порождают новые факторы экономического роста, в частности «электронный» менеджмент, позволяющий на основе использования интернет-технологий при сокращении штатов и улучшении менеджмента добиваться увеличения объемов производства и продаж, производительности труда, уменьшения производственных затрат. Это обеспечивает неинфляционный экономический рост, способствует повышению эффективности и устойчивости организаций.

Острая конкуренция, вызванная коротким жизненным циклом информационных продуктов, приводит к формированию олигопольной структуры информационной экономики. Традиционный принцип определения цены и объема производства путем выравнивания предельного дохода с предельными издержками при «электронно-сетевой» форме реализации экономических отношений существенно модифицируется, поскольку предельные издержки на производство дополнительной единицы продукции становятся ничтожно малы. В результате спрос и предложение ведут себя особым образом: повышение спроса, в частности, не приводит к росту цен. Примером является Интернет, подключение к которому все большего числа пользователей не влечет повышения тарифов, так как предельные издержки на подключение дополнительного пользователя близки или равны нулю. Вследствие этого отрасли экономики, связанные с производством телекоммуникационного оборудования, компьютеров, полупроводников и другого электронного оборудования, предоставлением услуг в

сфере коммуникаций, компьютерной техники и программного обеспечения, являются самыми быстрорастущими.

Социальная сфера жизнедеятельности общества определяется совокупностью отношений, связанных с организацией производительных сил. Влияние информационных технологий на социальную сферу проявляется по нескольким направлениям.

Во-первых, снижается влияние рабочего класса и нарастает дифференциация его структуры. С одной стороны, все большее число видов труда требует серьезной профессиональной подготовки, и соответственно занятым таким трудом работникам предъявляются все более высокие требования по интеллектуальным способностям и деловым качествам. В силу относительной редкости людей с необходимыми способностями и качествами, а также их заметного влияния на эффективность производственной деятельности их труд хорошо оплачивается. По своим жизненным стандартам и интересам, в том числе хозяйственным, они выходят за рамки традиционно понимаемого пролетариата. С другой стороны, отмеченные процессы порождают потребность в значительной массе людей, занимающихся низкоквалифицированным трудом как в материальном производстве, так и в сфере услуг. Эти люди вследствие определенных жизненных обстоятельств, в том числе связанных с обесцениванием их интеллектуальных способностей современной организацией труда, часто оказываются хронически безработными и ввиду этого не могут быть отнесены к пролетариату.

В обозначенных условиях позиции людей, входящих в низшую страту общества, весьма уязвимы, так как их единственным значимым ресурсом оказывается знание, которое не приобретается в ходе коллективных действий. Фактически единственным эффективным методом повышения благосостояния таких работников становится приобретение уникальных навыков, которое не может быть достигнуто легким путем.

Во-вторых, изменяется характер мотивов и стимулов, определяющих повседневную деятельность человека. Эти мотивы и стимулы во все большей мере трансформируются из внешних, задаваемых стремлением к росту материального благосостояния, во внутренние, порождаемые жаждой самореализации и личного роста. Подобное поведение предполагает большую степень духовной свободы человека, его самостоятельности и ответственности за свою судьбу.

В-третьих, происходит обособление новой технократической элиты постиндустриального общества на основе индивидуальных, личностных качеств человека. Эта страта общества объединяет прежде всего людей, воплощающих в себе знания и информацию о производственных процессах и механизмах общественного прогресса в целом. Такие люди привносят в процесс коллективного

принятия решений специальные знания, талант и опыт. Основанием для причисления этих специалистов к технократической элите становятся их способности к творческой деятельности, к усвоению, обработке и продуцированию информации и знаний.

По мере того как наука становится непосредственной производительной силой, роль технократической элиты возрастает. Ее представители обеспечивают производство уникальных благ, которые оказываются залогом процветания общества. В силу этого в распоряжение данной элиты переходит все большая часть общественного достояния. Тем не менее особо следует отметить, что способность продуцировать новые знания отличает людей друг от друга гораздо больше, чем масштаб личного материального богатства; более того, такая способность не может быть приобретена мгновенно и не подлежит радикальной корреляции. Поэтому эта страта общества имеет все шансы стать устойчивой социальной группой.

Сфера духовной жизни включает отношения, связанные с созданием, хранением и использованием объектов культуры общества, во многом определяющей интенсивность постиндустриального развития экономической и социальной сфер. Она охватывает области образования, воспитания, науки, искусства, религии, политики, массовой информации, литературы и др.

Современные информационные технологии существенно повышают эффективность интеллектуальной деятельности, в том числе проведение научных исследований, предоставляя невиданные ранее возможности сбора необходимой информации, ее обработки, анализа и синтеза вариантов решений сложных проблем во всех сферах общественной жизни.

Трудно переоценить значение этих технологий и для сохранения культурных ценностей. Они вносят значительные изменения в процесс обучения, его продолжительность, порядок осуществления и темпы, увеличивают возможности доступа к нему значительного числа людей. Особенно велико значение информационных технологий в дистанционном образовании, которое в настоящее время является наиболее стремительно развивающейся формой обучения во всем мире. Общество использует дистанционное образование в целях просвещения и подготовки большого числа людей при умеренных расходах, почти не нарушая при этом течения их жизни. Именно необходимость вовлечения в образовательный процесс большого количества людей выдвигает дистанционное образование на первое место среди образовательных систем ближайшего будущего. Эта потребность усиливается в результате изменений в характере работы и смещения акцентов с сельского хозяйства и промышленного производства в сторону сферы услуг, коммуникации и информационной индустрии, где необходимо постоянное обновление знаний и навыков.

Сфера государственного управления характеризуется совокупностью отношений, возникающих в процессе выполнения государством своих функций, которые в самом общем виде заключаются в обеспечении жизнедеятельности общества и его самосохранения как единого целого. Эти функции детализируются и развиваются в сложную систему более частных функций: охрана территориальной целостности, установление и охрана правового порядка, защита общества от внешних и внутренних угроз. Выполнение функции государства осуществляется специальным аппаратом государственной власти за счет средств, собираемых государством в виде налогов.

Воздействие информационных технологий на данную сферу жизни общества обусловлено тем, что эти технологии позволяют повысить эффективность информационной деятельности основных субъектов публичной власти. Они способствуют повышению оперативности получения сведений об основных характеристиках общественного развития, глубины и качества анализа этих сведений, подготовки и оформления решений, принимаемых органами государственной власти по управлению обществом, контроля выполнения принятых решений, а также оказания социальных услуг населению, включая предоставление доступа к открытым государственным информационным ресурсам.

Одной из наиболее развитых форм внедрения современных информационных технологий в процесс государственного управления является система «***электронного правительства***». Концептуально она представляет собой совокупность взглядов на использование современных информационных технологий для выполнения функций государства в условиях продолжающейся научно-технической революции в области вычислительной техники, коммуникации и связи.

Реализация концепции «электронного правительства» направлена на достижение следующих основных целей:

– повышение эффективности работы аппарата государственного управления на основе внедрения безбумажных технологий управления;

– стимулирование экономического развития посредством расширения доступа хозяйствующих субъектов к открытым государственным ресурсам;

– повышение качества жизни граждан посредством снижения социальных издержек при осуществлении информационного взаимодействия граждан с органами государственной власти;

– укрепление взаимодействия государства и общества по важнейшим проблемам жизнедеятельности социума на основе использования информационных технологий.

Таким образом, новое качество общественного развития, обусловленное использованием современных информационных техно-

логий, проявляется как результат преодоления природы традиционного способа производства на основе радикального ускорения технологического прогресса, относительного снижения роли материального производства, развития сектора услуг и информации, изменения мотивации и характера человеческой деятельности, превращения знаний в новый тип вовлекаемых в производство ресурсов, а также как результат существенной модификации социальной системы.

В исторической науке выделяют *три основных этапа развития цивилизации*: доиндустриальный; индустриальный; информационный (постиндустриальный).

Такая периодизация социального прогресса основана на нескольких важнейших параметрах:

– основной производственный ресурс (на доиндустриальном этапе — первичные условия производства — сырье, на индустриальном — энергия, на информационном — информация);

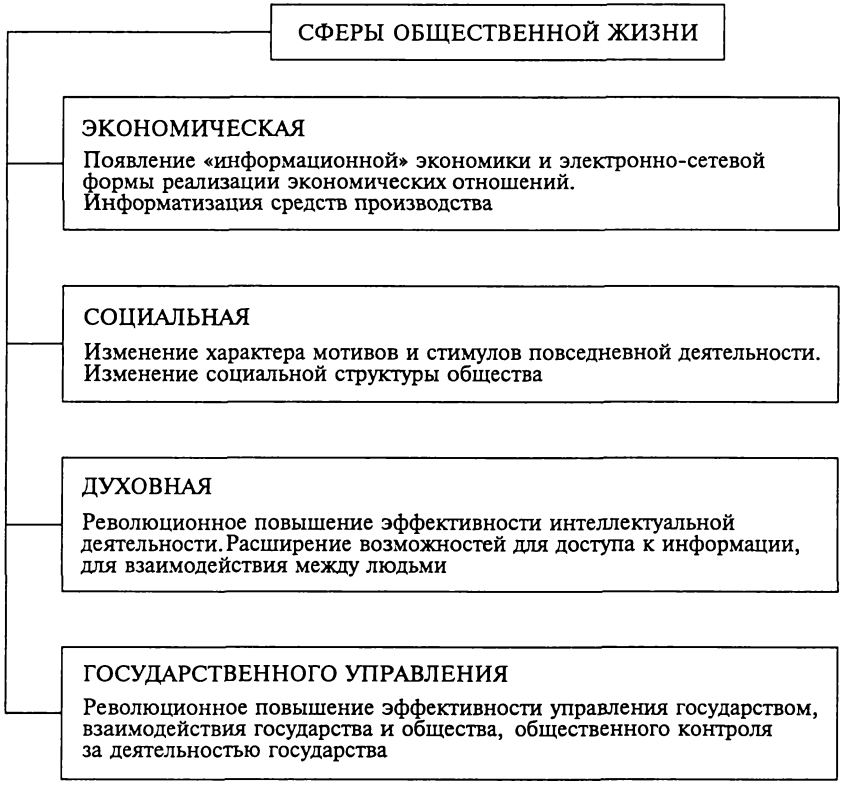


Рис. 1

– тип производственной деятельности (на доиндустриальном этапе — добыча, на индустриальном — изготовление, на информационном — обработка);

– характер базовых технологий производства (на доиндустриальном этапе — трудоемкие, на индустриальном — капиталоемкие, на информационном — наукоемкие).

Переход от одного этапа развития общества к другому, как правило, не имеет революционного характера и четкой хронологии: новые отношения относительно длительное время сосуществуют со старыми, усугубляя комплексность общества, усложняя социальную структуру и изменяя саму ее природу.

Основные характеристики информационного общества представлены на рис. 1.

1.2. Безопасность в информационном обществе

Информационные технологии, изменяя социальную организацию общества, не оказывают влияния на основные законы его развития, на природу человека, биологическую и психологическую основу его жизни. В связи с этим не претерпевают изменений и основные социальные источники угроз интересам человека, общества и государства, свойственные доиндустриальному и индустриальному этапам цивилизационного развития.

К числу таких источников угроз относится прежде всего конфликтное взаимодействие с другими субъектами жизни общества, обусловленное антагонистическими противоречиями в представлениях об объектах удовлетворения насущных нужд, потребностей и интересов, о способах овладения этими объектами и направлениях их использования.

Наиболее часто объектами конфликтных отношений становятся дефицитные материальные ресурсы (земля, вода, домашние и дикие животные, деньги, иные ограниченные ресурсы, являющиеся объектами собственности или государственного суверенитета), отношения власти, дающие возможность распоряжаться людьми и материальными объектами, духовные ценности (религиозные и культурные ценности, верования, особенности жизненного уклада, образа жизни, языковые и расовые отличия и т. п.).

Существенным отличием угроз, возникающих в информационном обществе, от угроз, характерных для индустриального общества, является изменение форм их проявления и способов реализации.

Так, преступления с корыстными целями, всегда представлявшие собой значительную социальную опасность, все чаще совершаются не только с применением современных информационных технологий, но и с использованием информации в качестве средства осуществления корыстных посягательств. По мере развития

«электронно-сетевой» экономики, информатизации государственных органов тенденция роста этого вида преступлений в ближайшем будущем, видимо, будет нарастать.

Все больший ущерб предпринимательской деятельности граждан и организаций, а также деятельности государственных органов наносят распространение в компьютерных сетях вредоносных программ (часто называемых вирусами), осуществление несанкционированного доступа к информационным ресурсам, распространение «информационной» макулатуры (спама).

Расширяется использование современных информационных технологий для совершения преступных деяний в области нарушения конституционных прав и свобод человека и гражданина, ведения экономического и промышленного шпионажа, раскрытия сведений, составляющих личную, семейную, коммерческую, государственную и другие охраняемые законом тайны.

Усиливается опасность использования современных информационных технологий для нанесения ущерба политическим, экономическим, военным и иным интересам государства со стороны террористических организаций и враждебных государств. Многие страны активно проводят исследования в области использования информационных технологий для оказания силового давления на политическое руководство противостоящих государств, совершенствуют методы и способы ведения так называемых информационных войн.

Все это выделяет обеспечение безопасности в качестве важнейшего направления деятельности человека, организаций и государственных органов в информационном обществе.

Важная особенность указанной деятельности — многообразие возможных объектов безопасности, проявлений угроз этим объектам и содержания последствий таких проявлений. Для эффективного обеспечения безопасности важно не только владеть необходимыми знаниями и навыками осуществления тех или иных конкретных мероприятий, использования средств и методов противодействия угрозам, но и обладать определенной теоретической подготовкой, позволяющей комплексно рассматривать возникающие в данной области вопросы применительно к любому объекту безопасности.

Контрольные вопросы

1. Что такое «информационное» общество?
2. Каким образом современные информационные технологии оказывают влияние на экономическую и духовную сферы жизни общества, на сферу государственного управления?
3. Чем обусловлена актуальность проблемы обеспечения безопасности в информационном обществе?

Глава 2

ИНФОРМАЦИЯ — ФАКТОР СУЩЕСТВОВАНИЯ И РАЗВИТИЯ ОБЩЕСТВА

2.1. Информация как явление жизни

Понятие «информация» — одно из базовых понятий теории обеспечения информационной безопасности. Объем явлений, охватываемых этим понятием, во многом определяет предмет обеспечения безопасности, характер угроз и методы противодействия этим угрозам.

В настоящее время отсутствует общепринятое представление о том, что такое информация. Однако критический анализ известных определений позволяет считать, что ***информация*** — это явление жизни организмов, заключающееся в отражении окружающей действительности для оценки происходящих в ней изменений и выбора системы действий по приспособлению к этим изменениям.

Каждый тип организма обладает свойственной только ему совокупностью средств адаптации к изменениям окружающей действительности, что позволяет в определенных пределах обеспечивать приемлемые условия для протекания биохимических процессов, составляющих сущность организма. Уникальность средств адаптации каждого типа организмов обусловливает, в свою очередь, уникальность его «информационного» взгляда на мир, во многом не пересекающегося с «мировоззрением» других видов организмов.

По содержанию ***информация*** — это результат отображения в организме движения объектов окружающей действительности, включающей как материальную, так и нематериальную составляющие.

Известно[1], что материя в качестве субстанции выступает как объективная реальность, рассматриваемая со стороны ее внутреннего единства, безотносительно ко всем тем бесконечно многообразным видоизменениям, в которых она существует.

К числу самых важных категорий философии, обозначающих атрибуты материи, относят движение, отражение и взаимодействие.

Категория «*движение*» в материалистической философии определяет различные типы изменчивости, наблюдаемые в объектив-

---

[1] *Алексеев П. В., Панин А. В.* Диалектический материализм. — М.: Высш. шк., 1987. — С. 94.

ном мире начиная от перемещения объектов в пространстве и кончая процессами биологической и социальной эволюции. Категория «*отражение*» охватывает проявления свойства одних объектов материального мира воспроизводить в их природе особенности других взаимодействующих с ними объектов[1], т.е. свойства сохранять «следы» некоторых характеристик объектов взаимодействия. Наконец, категория «*взаимодействие*» описывает явления взаимного изменения объектов материального мира в процессе их движения.

Отражение взаимосвязано с взаимодействием и движением. Везде, где имеет место движение и взаимодействие, присутствует отражение.

В философии принято различать отражение в неживой и живой природе. В неживой природе отражение носит пассивный характер. Оно проявляется в виде соответствующих изменений физических или химических свойств и состояний объектов, происходящих в результате внешнего воздействия. Отражение движения объектов материального мира в организмах, как было отмечено ранее, связано с изменением происходящих в них биохимических преобразований. Продукты измененных биохимических преобразований составляют материальную основу результата отражения движения в организмах, т.е. информации, а отраженный в организме образ действительности — его нематериальную основу.

В мире взаимодействующих организмов информация проявляется в форме сведений и в форме сообщений.

Сведения представляют собой результат отражения окружающей действительности в организме.

Как уже было отмечено, каждый тип организмов обладает определенной, свойственной только ему «*информационной*» *моделью мира*. Эта модель возникает на основе обобщения сведений, отражаемых и накапливаемых организмом. Получаемые организмом сведения служат, с одной стороны, для формирования и актуализации «информационной» модели, выявления изменения состояния объектов материального мира, а с другой — для оценки возможных последствий выявленных изменений для существования организма и выбора рационального «варианта поведения». Структура «информационной» модели определяется генотипом организма. В наиболее простом виде данная модель включает отражаемые объекты реального мира, характеристики их состояния, оценки возможного влияния состояния этих объектов на жизнедеятельность организма, набор вариантов «поведения» организма в ситуациях, требующих реагирования, а также отношения (связи) меж-

---

[1] *Алексеев П. В., Панин А. В.* Диалектический материализм. — М.: Высш. шк., 1987. — С. 150.

ду характеристиками состояния отражаемых объектов и вариантами «поведения».

Можно предположить, что «информационная» модель организмов, не обладающих большим разнообразием вариантов адаптации к изменениям окружающей действительности, имеет жесткую структуру, которая остается неизменной в течение их жизни. Структура «информационной» модели организмов с достаточным разнообразием таких вариантов является гибкой, т.е. в определенных пределах может изменяться, накапливая сведения об окружающем мире.

Организмы, обладающие развитой нервной системой и психикой, имеют более широкие возможности как по модификации структуры «информационной» модели, так и по оперированию с содержащимися в ней сведениями. В частности, эти организмы способны вырабатывать ***знания***, представляющие собой специфический вид сведений, отражающих закономерности изменения окружающей действительности и результативности использования имеющихся средств адаптации к данным изменениям. Специфика знаний заключается в том, что они являются результатом не непосредственного отражения движения каких-либо объектов действительности, а обобщения сведений о движениях этих объектов, накопленных в «информационной» модели. Знания позволяют организму прогнозировать на основе отражения реальной действительности позитивные и негативные последствия происходящих изменений или осуществляемых действий, что существенно повышает возможности его «комфортного» существования и выживания. Можно предположить, что способность выявления знаний появляется у организмов тогда, когда число возможных вариантов «поведения» становится значительным и их рефлекторное использование не позволяет обеспечить приемлемую эффективность адаптации.

Исключительно важную, с рассматриваемой точки зрения, часть живого мира образуют ***социальные организмы***, условием существования которых является взаимодействие с другими такими же организмами. Их «информационные» модели, кроме сведений, получаемых самостоятельно, включают сведения, поступающие от других членов социума. Способность обмениваться сведениями реализуется через отправку и получение информации в форме сообщений.

Сообщение представляет собой набор знаков, с помощью которых сведения, накопленные одним организмом, могут быть переданы другому организму и восприняты им.

Способность обмениваться информацией реализуется организмами путем определенных алгоритмов кодирования сведений, т.е. превращения их в набор знаков, воспринимаемых другими организмами и составляющих содержание сообщений, и алгоритмов

декодирования поступающих сообщений, т.е. превращения набора знаков в сведения. При этом совершенно несущественно, каким именно способом осуществляется передача сообщения и какой набор знаков использован для его формирования.

Сведения, получаемые организмом от других организмов, образуют *социальную составляющую* его «информационной» модели мира, а совокупность этих составляющих «информационных» моделей взаимодействующих организмов — распределенную «информационную» модель социума, его «коллективный разум».

Одними из социальных организмов, существующих на Земле, являются человек и общество, которые обладают способностью отражать окружающую действительность в своей «информационной» модели мира в виде сведений, накапливать сведения, обобщать их и формировать знания, а также обмениваться сведениями с другими людьми и обществами.

С этой точки зрения информация представляет собой явление жизни и человека и общества, важнейший фактор их существования.

Информация в выделенных формах обладает во многом отличающимися свойствами, содержание которых отражено на рис. 2.

Приведенная трактовка сущности, содержания и форм информации не противоречит тому, как это понятие раскрывается в обыденной жизни и в праве. Так, в справочной литературе под информацией понимается «информирование о положении дел в какой-либо области, о каких-либо событиях; сообщение о положении дел где-либо, о каких-либо событиях; сведения об окружающем мире и протекающих в нем процессах, воспринимаемые человеком или специальными устройствами»[1]. В федеральном законодательстве дефиниция «информация» раскрывается как «сведения (сообщения, данные) независимо от формы их представления»[2]. Понятие «данные» можно рассматривать как разновидность сообщений, предназначенных для автоматизированной обработки с использованием средств вычислительной техники. Эти сведения (сообщения, данные) могут отражать характеристики состояния объектов (лиц, предметов, фактов, событий) или движения конкретных объектов (явлений, процессов) окружающей действительности.

Не умаляя фундаментального характера теории информации, разработанной К. Шенноном, и методологического подхода к ис-

---

[1] Современный толковый словарь русского языка. — СПб.: «Норит», 2003. — С. 248.

[2] Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27 июня 2006 г.

Рис. 2

следованию окружающей действительности, составляющего основу разработанной Н. Винером кибернетики, можно отметить, что используемая ими концепция «информации» ограничивается рассмотрением только той составляющей этого явления, которая имеет форму сообщений[1]. Применительно к ней раскрываются закономерности, связывающие количество двоичных знаков (битов), достаточных для описания одной буквы или знака сообщения (количество информации), с пропускной способностью канала связи, характеризуемой максимальным количеством информации (битов, достаточных для описания одного знака), которое можно передать по нему за одну секунду.

Вообще говоря, между количеством информации по К. Шеннону (т.е. количеством битов, достаточных для передачи одного знака сообщения) и количеством сведений (т.е. количеством новых элементов «информационной» модели человека, которые возникают вследствие осознания им сообщения) трудно установить какое бы то ни было соотношение. Единственное, что можно в

[1] *Стрельцов А.А.* Обеспечение информационной безопасности России. Теоретические и методологические основы. — М.: МЦНМО, 2002.

связи с этим отметить: если предположить, что каждый бит соответствует некоторому знаку, а знак, в свою очередь, — элементу части передаваемой «информационной» модели, то количество информации по К. Шеннону позволяет оценить количество знаков, достаточных для кодирования этой части модели.

Теория информации К. Шеннона безусловно вскрыла ряд объективных закономерностей природы. В процессе развития этой теории последователями Шеннона произведено существенное расширение трактовки понятия «информация». «У большинства из тех, кто думал над этим кругом проблем, возникло предчувствие, что достаточно сделать небольшое обобщение, похожее на сделанное в свое время обобщение понятия энергии, и термин «информация» поможет установить какую-то глубинную закономерность нашего мира, эквивалентную по своему познавательному значению закону сохранения энергии»[1]. К сожалению, этого пока не произошло.

Другим выдающимся достижением, оказавшим существенное влияние на превращение понятия «информация» в общенаучную категорию, были разработанные Н. Винером основы кибернетики. Введенный им термин «кибернетика» был предназначен для обозначения всей теории управления и связи в машинах и живых организмах[2]. В рамках этой работы Н. Винер также пришел к понятию количества информации, но в результате изучения не проблем кодирования информации, а проблем сообщений и шумов в электрических фильтрах.

Наиболее известным научным результатом работы Н. Винера можно считать открытие достаточно широкого класса задач, связанных с поддержанием целенаправленного функционирования динамических объектов, а также метода «управления с помощью информирующей обратной связи», используемого в этих объектах[3]. Существо этого метода в упрощенном виде может быть сформулировано как использование при управлении не только сведений о том, как должен двигаться управляемый объект, но и сведений о том, как он двигается к поставленной цели на самом деле. Для этого оцениваются отклонения параметров движения объекта от требуемых значений, на основе которых формируются управляющие воздействия на движущие элементы объекта в целях внесения требуемых изменений в это движение. Для реализации данного метода требуется наличие системы связи, передающей сообщения от управляющего центра к управляемым движителям и обратно, что, естественно, требует исследования и собственно сообщений.

---

[1] *Тростников В. Н.* Человек и информация. — М.: Наука, 1970. — С. 183.

[2] *Винер Н.* Кибернетика, или управление и связь в животном и машине. Вторая редакция. — М.: Наука, 1983. — С. 57.

[3] Там же. — С. 183.

Объекты, в которых используется указанный метод управления, как правило, описываются линейными дифференциальными уравнениями, решения которых инвариантны к временным сдвигам. Широкая распространенность таких объектов в реальной жизни обусловила и большую востребованность кибернетических идей и методов при решении практических задач в различных сферах человеческой деятельности[1].

В то же время между управлением в технических системах и управлением в биологических и социальных системах наряду с наличием общих черт существуют и определенные различия. В биологических и социальных системах, как следует из вышеизложенного, управление осуществляется с использованием сведений, а в технических системах — с использованием сообщений. Вследствие этого управление в биологических и социальных системах не имеет той жесткости, которая свойственна управлению в технических системах. Если в технической системе для оказания управляющего воздействия достаточно отправить сообщение или сигнал, то в биологических и социальных системах этого не всегда достаточно. Это особенно наглядно проявляется на примере социальных систем, в которых для реализации управляющего воздействия, как правило, требуется приложить определенные дополнительные усилия, чтобы индивиды, составляющие социальную систему, согласились выполнять такое управляющее воздействие.

Если в качестве управляемого объекта выступают отдельные органы человеческого организма, то управление практически не отличается от аналогичного процесса в технических системах. Это обусловлено особенностями человеческого организма, которые заключаются в том, что все его внутренние органы работают, как правило, независимо от сознания и с точки зрения управления образуют самостоятельные биологические системы со своей «информационной» моделью, слабо связанные с «информационной» моделью, используемой сознанием человека. Система управления такими органами и была выбрана Н.Винером в качестве объекта исследования. Если бы в качестве объекта исследования выступало сознание, то система управления выглядела бы значительно сложнее.

2.2. Информационная инфраструктура

Передача сообщений через естественную среду обитания — воздух — обеспечивает обмен сведениями между индивидами, однако обладает рядом объективных ограничений по дальности и оперативности осуществления информационного обмена, по длитель-

[1] *Черри К.* Человек и информация. Критика и обзор. — М.: «Связь», 1972.

ности хранения переданных сообщений и возможности их ретроспективного анализа. Эти ограничения, в свою очередь, сказываются на активности информационного взаимодействия между индивидами и, соответственно, на развитии социума, использовании имеющихся у него ресурсов и сил для адаптации к изменяющимся условиям существования.

Преодоление выделенного ограничения связано с созданием искусственной среды передачи информации, которая придает процессу информационного взаимодействия новое качество. Способность организмов создавать такую искусственную среду существенно зависит от имеющихся у них средств воздействия на окружающую действительность и от способности использовать коллективные действия для повышения эффективности адаптации.

Наибольшими возможностями осуществления подобной деятельности обладает человек. Можно сказать, что если информация — явление жизни человека и общества, то ***информационная инфраструктура*** — это явление социальной жизни индивидов. *Сущность* данного явления заключается в разрешении противоречия между социально обусловленными потребностями в информационном обмене между членами общества для решения задач экономического, социального, политического и духовного развития и исторически обусловленными социальными и техническими возможностями удовлетворения этих потребностей.

Содержание данного явления общественной жизни определяется совокупностью используемых обществом информационных технологий и технических систем, реализующих эти технологии, а также совокупностью социальных институтов, обеспечивающих создание, эксплуатацию и модернизацию технических систем обеспечения информационного взаимодействия.

Ключевым элементом информационной инфраструктуры, во многом определяющим ее содержание, являются *информационные технологии*. Под информационной технологией понимается упорядоченная совокупность методов обработки сообщений, включающих поиск, сбор, хранение, передачу и распространение сообщений, а также их предоставление человеку.

Информационная инфраструктура по форме — это совокупность социально-технических систем, реализующих функции обеспечения информационного взаимодействия, и общественно поддерживаемого порядка использования данных систем в жизни человека и общества.

В информационной инфраструктуре современного общества выделяют три основных сегмента: субъектный, общественный и смешанный.

Субъектный сегмент ориентирован на обеспечение информационного обмена в интересах отдельных субъектов информацион-

ной сферы и образуется инфраструктурами сетей связи и информатизации индивидуального пользования.

Сети связи представляют собой технологические системы, включающие средства и линии связи и предназначенные для осуществления электросвязи или почтовой связи[1]. Понятие «электросвязи» раскрывается в законодательстве как «любые излучения, передача или прием знаков, сигналов, голосовой информации, письменного текста, изображений, звуков или сообщений любого рода по радиосистеме, проводной, оптической и другим электромагнитным системам»[2]. Дефиниция «почтовая связь» в законодательстве определена как «вид связи, представляющий собой единый производственно-технологический комплекс технических и транспортных средств, обеспечивающий прием, обработку, перевозку, доставку (вручение) почтовых отправлений, а также осуществление почтовых переводов денежных средств»[3].

Особое значение для удовлетворения потребностей общества в информационном обмене имеет *федеральная связь*, объединяющая все организации и государственные органы, осуществляющие и обеспечивающие электросвязь и почтовую связь на территории Российской Федерации[4].

Можно сказать, что в рамках сети связи сосредоточены все основные технологические средства передачи информации в форме сообщений в интересах граждан, субъектов, представляющих социальные институты общества, государственных органов.

Инфраструктура информатизации индивидуального пользования призвана обеспечить «организационный социально-экономический и научно-технический процесс создания оптимальных условий для удовлетворения информационных потребностей и реализации прав граждан, органов государственной власти, органов местного самоуправления, организаций, общественных объединений на основе формирования и использования информационных ресурсов»[5]. Она определяется совокупностью информационных технологий, информационных ресурсов и систем, средств, обеспечивающих возможность использования информационных ресурсов и систем субъектами информационной сферы, систем автоматизированного управления, систем автоматизации производства, а также кадров, обеспечивающих их эксплуатацию. При этом технологическую основу инфраструктуры информатизации субъектов составляют информационные ресурсы, информационные технологии и

---

[1] Федеральный закон «О связи» от 18 июня 2003 г. Ст. 2.

[2] Там же. Ст. 2.

[3] Федеральный закон «О почтовой связи» от 17 июля 1999 г. Ст. 2.

[4] Федеральный закон «О связи» от 18 июня 2003 г. Ст. 11, п. 1.

[5] Федеральный закон «Об информации, информатизации и о защите информации» от 20 февраля 1995 г. Ст. 2.

телекоммуникационные системы, обеспечивающие возможность удаленного доступа субъектов к информационным ресурсам и системам.

Общественный сегмент информационной инфраструктуры ориентирован на обеспечение информационного обмена в интересах общества и государства и образуется инфраструктурами средств массовой информации и информатизации общего пользования.

Средства массовой информации представляют собой «периодическое печатное издание, радио-, теле-, видеопрограмму, кинохроникальную программу, иную форму периодического распространения массовой информации», т.е. печатных, аудио-, аудиовизуальных и иных сообщений и материалов, предназначенных для неограниченного круга лиц[1]. При этом под массовой информацией понимаются «предназначенные для неограниченного круга лиц печатные, аудио-, аудиовизуальные и иные сообщения и материалы», а под периодическим печатным изданием — «газета, журнал, альманах, бюллетень, иное издание, имеющее постоянное название, текущий номер и выходящее в свет не реже одного раза в год». Другими словами, средства массовой информации есть издание (радио-, теле-, видеопрограмма, кинохроникальная программа, иная форма периодического распространения массовой информации), отличающееся наличием трех признаков: постоянным названием, текущим номером и определенной периодичностью выхода в свет.

Средства информатизации общего пользования образуются совокупностью открытых информационных ресурсов библиотек, архивных и музейных фондов, а также открытых государственных информационных ресурсов, обеспечивающих свободный доступ граждан к сведениям о деятельности государственных органов, к публикуемым ими нормативным правовым актам и другой общественно значимой информации.

Смешанный сегмент информационной инфраструктуры представляет собой совокупность инфраструктур глобальных информационно-телекоммуникационных систем.

Основной составляющей смешанного сегмента информационной инфраструктуры являются *глобальные информационно-телекоммуникационные системы* (например, система Интернет) — совокупность средств связи и информатизации, предназначенных как для обеспечения информационного взаимодействия между конкретными субъектами, так и для распространения массовой информации для неограниченного круга лиц.

Функциональные возможности данного сектора информационной инфраструктуры определяются, с одной стороны, имею-

[1] Закон Российской Федерации «О средствах массовой информации». Ст. 2.

щимися в его составе средствами получения и передачи сообщений между отдельными субъектами, сбора и хранения полученной информации, а с другой — средствами производства и распространения массовой информации посредством установления информационного взаимодействия отдельного субъекта с неограниченным количеством других субъектов.

Основные сегменты информационной инфраструктуры представлены на рис. 3.

Общей особенностью использования средств информационной инфраструктуры для осуществления информационного взаимодействия является наличие посредника между субъектами, устанавливающими информационное взаимодействие.

В качестве такого посредника могут выступать конкретные физические или юридические лица (посыльный, фельдъегерская служба, телефонная компания), выполняющие функции либо установления информационного взаимодействия, либо предоставления возможности для информационного взаимодействия. Данное обстоятельство обусловливает возникновение определенных общественных отношений между посредником и обслуживаемыми им субъектами.

С появлением электрической связи, развитием глобальных информационно-телекоммуникационных систем функции посредника все больше смещаются в сторону предоставления возможностей информационного взаимодействия.

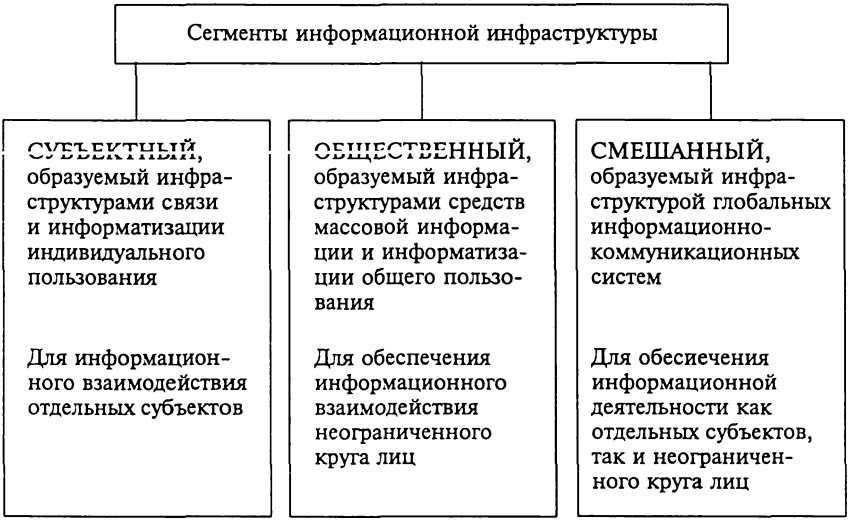


Рис. 3

Контрольные вопросы

1. Что такое информация?
2. Каковы основные формы и свойства информации?
3. Что такое информационная инфраструктура?
4. Каковы основные составляющие информационной инфраструктуры?

Глава 3

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ: СОДЕРЖАНИЕ И СТРУКТУРА ПОНЯТИЯ

3.1. Обеспечение безопасности

Понятие «обеспечение информационной безопасности» описывает совокупность явлений, охватываемых понятиями «обеспечение безопасности» и «информационная безопасность».

Понятие «обеспечение» в русском языке трактуется двояко: один из видов деятельности; средство деятельности. Как вид деятельности обеспечение означает совокупность действий, предпринимаемых для того, чтобы сделать нечто «вполне возможным, действительным, реально выполнимым»[1], а как средство деятельности — «то, чем обеспечивают кого-нибудь или что-нибудь»[2].

Деятельность как особый способ существования человека, выделяющий его на фоне других живых существ, может быть представлена в виде совокупности продолжающихся в течение длительного времени действий, направленных на достижение определенной цели, результата. Основным субъектом деятельности выступает индивид[3], который таким способом удовлетворяет свои потребности в необходимых условиях существования.

Индивид может осуществлять деятельность по достижению стоящих перед ним целей один или совместно с другими индивидами. При этом деятельность привлекаемых индивидов направлена на достижение цели, которая ими не ставилась и к удовлетворению их потребностей и интересов прямого отношения не имеет. Это отношение к цели привлекаемых индивидов составляет существо обеспечения как вида деятельности. Например, деятельность по получению удостоверения депутата Государственной думы предполагает не только собственно подачу необходимых документов в избирательную комиссию, но и осуществление агитационной работы, мониторинга социально-политической ситуации, подготовку и грамотное использование необходимых финансовых и материальных средств, «борьбу» с другими кандидатами за голоса избирателей, т. е. осуществление целого ряда мер, способных привести к получению статуса депутата.

Структура понятия *обеспечение* помимо самой деятельности по обеспечению включает средства и субъектов обеспечения.

---

[1] *Ожегов С. И.* Словарь русского языка. — С. 364.

[2] Там же. — С. 364.

[3] Обществознание / отв. ред. М. Н. Марченко. — М.: Зерцало, 2001. — С. 58.

Деятельность по обеспечению заключается в оказании помощи субъектам в достижении поставленных ими целей.

Средства обеспечения образуются совокупностью материальных, духовных, финансовых, правовых, организационных и технических средств, необходимых для осуществления деятельности по обеспечению.

Обеспечение как вид деятельности осуществляется определенными субъектами — индивидами, негосударственными организациями и государственными органами.

Несмотря на то что основным субъектом деятельности выступает отдельный индивид, трудно отрицать, что его потребности и интересы во многом обусловлены социальными условиями существования и теми людьми, с которыми он взаимодействует. В процессе этого взаимодействия возникают общие потребности, интересы и мотивы деятельности *группы людей*, объединенных определенными отношениями, которые могут рассматриваться в качестве потребностей, интересов и мотивов действий данной группы. Физически носителями этих потребностей выступают отдельные индивиды, но свобода их деятельности существенно ограничена отношениями внутри группы, установленными в ней правилами поведения. В этой деятельности они проявляются как единый субъект с совпадающими потребностями, интересами и мотивами. Примером может служить хорошо сыгранная спортивная команда.

Деятельность группы людей по достижению конкретной цели или удовлетворению потребности также может предполагать соответствующее обеспечение. Так, оркестр, зарабатывающий на жизнь концертной деятельностью, нуждается в том, чтобы кто-нибудь позаботился о заказе и своевременности предоставления транспортных средств, о бронировании гостиниц, продаже билетов на концерты, об аренде концертных залов и т.д. Все вышеперечисленное не имеет прямого отношения к творческой деятельности, которой занимаются дирижер и музыканты, но без этой вспомогательной деятельности оркестр был бы вынужден давать концерты на улице.

Аналогичным образом можно рассматривать деятельность той или иной *социальной общности*, представляющей собой самодостаточную группу людей, способную собственной деятельностью создавать и воссоздавать все необходимые условия для совместной жизни. В той мере, в которой каждый индивид испытывает потребность в существовании, развитии и процветании данной общности и участвует в реализации возникающих в связи с этим интересов, можно полагать, что общность обладает потребностями и интересами. Примером обеспечения деятельности социальной общности могут служить известные факты из истории отношений между метрополией и колониями.

Особой разновидностью субъектов деятельности является *государство*, представляющее собой центральный институт политической системы общества. Его деятельность направлена на управление делами общества и обусловливается потребностями и интересами граждан, общественных организаций и элиты, возглавляющей государство и имеющей возможность применять власть. Обеспечение деятельности государства заключается в содействии правомерной деятельности граждан и деятельности должностных лиц, возглавляющих органы государственной власти. Обеспечение деятельности последних возлагается на аппарат соответствующих государственных органов.

Обеспечение как средство деятельности, т.е. «то, чем обеспечивают кого-нибудь или что-нибудь», представляет собой совокупность материальных и духовных объектов, финансовых, правовых и организационных средств, которые повышают эффективность деятельности по достижению целей. Его конкретное содержание определяется предметной сферой обеспечения как вида деятельности. Так, для обеспечения концертной деятельности оркестра необходимы транспортные средства, средства связи, гостиницы, концертные залы и т.д.

Цель основной деятельности может заключаться в поддержании устойчивого развития общества, в достижении и сохранении высокого уровня благосостояния его членов. Тогда обеспечение достижения этой цели представляет собой соответствующее управление процессами общественного развития, если под ним понимать «командный механизм общественной системы»[1]. Это обеспечение включает ряд функций государства, к наиболее важным из которых относят экономическую, социальную, развитие научно-технического прогресса, культуры и искусства, охраны правопорядка и укрепления законности, экологическую, поддержание взаимовыгодной международной торговли и мира, укрепление обороноспособности[2].

Цель основной деятельности может заключаться в исполнении государственного бюджета, принятого законодательной властью. Обеспечение достижения данной цели, состоит в осуществлении органами исполнительной власти таких мероприятий, которые будут способствовать достижению основных параметров бюджета. Эта деятельность отнесена Конституцией Российской Федерации к одной из самых важных функций Правительства[3].

Цель основной деятельности может состоять в автоматизации решения на предприятии некоторой задачи управления произ-

[1] *Кинг А., Шнайдер Б.* Первая глобальная революция. Доклад Римского клуба. — М.: Прогресс, 1991. — С. 232—233.

[2] *Сырых В.М.* Теория государства и права / отв. ред. С.А.Чибиряев. — М.: Былина, 1998. — С. 29—36.

[3] Конституция Российской Федерации, 1993. Ст.114 а).

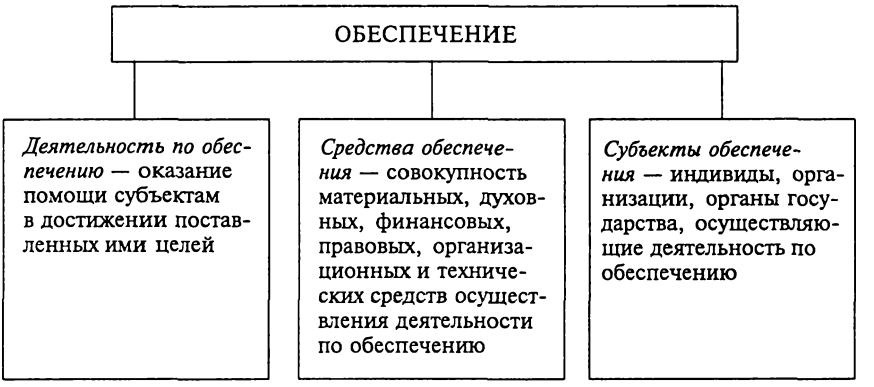


Рис. 4

водством. Тогда ее обеспечение будет включать создание необходимой технической основы (техническое обеспечение), программ (программное обеспечение), систематизированных наборов данных (информационное обеспечение), языковых средств взаимодействия пользователя с техническими и программными средствами (лингвистическое обеспечение), набора нормативных документов, определяющих порядок взаимодействия с системой и поддержания ее работоспособности (нормативное обеспечение)[1].

Если в качестве предмета обеспечения выступает выполнение некоторым должностным лицом (в том числе государственным) возложенных на него обязанностей, то обеспечение будет заключаться в определении структуры соответствующего аппарата, его кадровом наполнении, осуществлении определенной организационной, хозяйственной, информационно-аналитической и другой необходимой деятельности.

Общая структура понятия «обеспечение» представлена на рис. 4.

Понятие «*безопасность*» в русском языке определяется как «отсутствие опасности»[2], «состояние, при котором не угрожает опасность, есть защита от опасности»[3], понятие «*опасность*» означает «возможность, угрозу чего-нибудь опасного, т. е. способного причинить какой-нибудь вред, несчастье»[4], а понятие «*угроза*» — «возможную опасность, запугивание, обещание причинить кому-нибудь неприятность, зло»[5]. Таким образом, ***безопасность*** есть невозможность нанесения вреда кому-нибудь или чему-нибудь вследствие проявления угроз, т. е. их защищенность от угроз.

---

[1] Автоматизация управления / под ред. В.А.Абчука. — М.: Радио и связь, 1984.

[2] *Даль В.* Толковый словарь живого великорусского языка. М., 1989. — С. 67.

[3] *Ожегов С. И.*, Словарь русского языка. — М., 1990. — С. 67.

[4] Там же. — С. 388.

[5] Там же. — С. 716.

В структуре понятия «безопасность» выделяются объект безопасности, угрозы этому объекту и обеспечение его безопасности от проявления угроз (рис. 5).

Сущность понятия «***объект безопасности***» во многом определяет содержание явления «безопасность», обусловливая возможные угрозы и соответственно характеристики состояния защищенности от угроз. *Безопасность объекта* проявляется через безопасность его наиболее важных свойств или свойств структурных составляющих.

В данном контексте в качестве основных объектов безопасности рассматриваются организации, включая предприятия, и государство.

Под *организацией*, если не будет указано иное, понимается социальное объединение граждан, созданное для достижения определенных целей и имеющее определенную структуру.

Структура организации характеризуется степенью централизации (т. е. количеством уровней иерархии управления), степенью специализации обязанностей участников организации, уровнем стандартизации деятельности по координации, контролю и правилам проведения мероприятий, необходимых для достижения целей организации.

Существует значительное количество способов классификации организаций: по формализации отношений внутри организации (формальная, неформальная), по источникам финансирования их деятельности (бюджетная и внебюджетная), по членству (общественная, государственная, межгосударственная), по видам деятельности (по промышленному развитию, по добыче угля и т. п.).

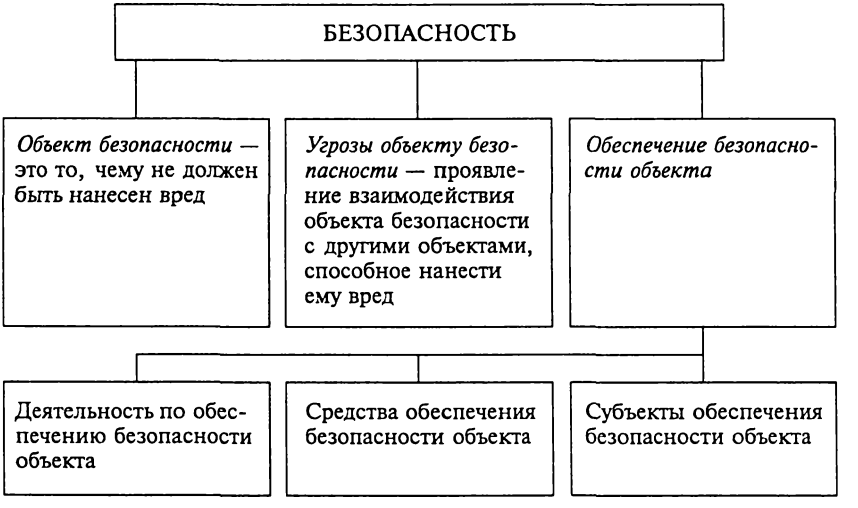


Рис. 5

По формам реализации гражданских прав организации могут образовывать или не образовывать юридическое лицо.

Юридическим лицом признается организация, которая имеет в собственности, хозяйственном ведении или оперативном управлении обособленное имущество и отвечает по своим обязательствам этим имуществом; она может от своего имени приобретать и осуществлять имущественные и личные неимущественные права, нести обязанности, быть истцом и ответчиком в суде[1].

Юридические лица обязаны иметь самостоятельный баланс или смету. Они могут иметь гражданские права, соответствующие целям деятельности, предусмотренным в его учредительных документах, и нести связанные с этим обязанности.

Юридическими лицами могут быть организации, преследующие извлечение прибыли в качестве основной цели своей деятельности (коммерческие организации) либо не имеющие извлечение прибыли в качестве такой цели и не распределяющие полученную прибыль между участниками (некоммерческие организации)[2].

Юридические лица, являющиеся *коммерческими организациями*, могут создаваться в форме хозяйственных товариществ и обществ, производственных кооперативов, государственных и муниципальных унитарных предприятий. Юридические лица, являющиеся *некоммерческими организациями*, могут создаваться в форме потребительских кооперативов, общественных или религиозных организаций (объединений), финансируемых собственником учреждений, благотворительных и иных фондов, а также в других формах, предусмотренных законом. Допускается создание объединений коммерческих и (или) некоммерческих организаций в форме ассоциаций и союзов.

Одной из форм коммерческих организаций являются *унитарные предприятия*, которые в отличие от других коммерческих организаций не наделяются правом собственности на закрепленное за ними имущество.

Содержание безопасности организации заключается в защищенности от угроз ее деятельности по достижению целей, определенных в уставных документах, и законных интересов, а также ее имущества, имущественных и личных неимущественных прав.

Безопасность организации оценивается величиной рисков ее деятельности. Величина риска определяется ожидаемой опасностью наступления неблагоприятных последствий, обусловленных проявлением угроз деятельности организации.

Другой важный объект безопасности — государство. Оно представляет собой особую форму реализации социальной власти, ба-

---

[1] Гражданский кодекс Российской Федерации. Ст. 48.

[2] Там же. Ст. 50.

зирующейся на урегулированных правом властных отношениях с другими субъектами общественной жизни. Социальная власть является структурной основой любой более или менее устойчивой и целенаправленной общности людей, обеспечивая ей целостность, устойчивость и управляемость.

Государство — это организация политической власти, охватывающая определенную территорию и выступающая одновременно как средство обеспечения интересов всего общества и как особый механизм управления и подавления.

Государство характеризуют следующие признаки:

– наличие публичной власти, реализуемой посредством специального аппарата государственных служащих;

– система налогов, податей, займов, необходимых для проведения государственной политики и содержания государственного аппарата;

– наличие территории, на которой реализуется государственная власть;

– легитимность, обусловливаемая существованием и действием права;

– монополия на применение силы, физического принуждения;

– суверенитет, заключающийся в возможности реализации властных полномочий на всей территории.

Государство в рамках осуществления власти выполняет вполне определенные функции, к наиболее важным из которых относятся:

– охрана прав и свобод человека и гражданина;

– выработка основных направлений социально-экономического развития общества и использование механизмов и ресурсов государственной власти для их реализации;

– налогообложение граждан и организаций, иных лиц, осуществляющих незапрещенную законом деятельность на управляемой территории;

– социальная защита населения;

– обеспечение обороны страны и безопасности государства;

– некоторые другие.

Угрозы государству могут проявляться в процессе взаимодействия, прежде всего, с другими государствами или с социальными группами. Это взаимодействие может как способствовать укреплению органов государственной власти, исполнению ими функций управления делами общества, так и ослаблять эти органы, затруднять реализацию возложенных на них функций. Так, длительное время наиболее опасной угрозой безопасности многих государств мира являлась возможность развязывания Третьей мировой войны, возникшая в результате взаимодействия наиболее развитых стран Запада и СССР. В современных условиях наиболее опасная угроза безопасности государств — международный тер-

роризм, сепаратизм и организованная преступность. Опасность выделенных угроз для развития государств, составляющих международное сообщество, неоднократно отмечалась в резолюциях Генеральной Ассамблеи Организации Объединенных Наций.

Угрозы безопасности государства могут порождаться в процессе взаимодействия общества с различными социальными группами и организациями (криминальными структурами, националистическими и некоторыми религиозными организациями), имеющими антагонистические интересы. Реализация этих интересов может привести к возрастанию социальной напряженности в обществе, усложнению решаемых государством задач управления делами общества, уменьшению его возможностей по решению этих задач.

3.2. Информационная безопасность и ее обеспечение

Как было отмечено ранее, безопасность проявляется через отсутствие вреда функционированию и свойствам объекта либо его структурным составляющим. Это положение служит методологическим основанием для выделения видов безопасности, в частности информационной безопасности.

Одна из важных структурных составляющих выделенных объектов безопасности — информация или деятельность, предметом которой является информация. Наличие угроз этим объектам позволяет говорить об их информационной безопасности — безопасности их «информационного измерения».

Свое ***«информационное измерение»*** присуще ***человеку***, в существовании которого информация играет такую же важную роль, как пища, воздух, вода. Она обусловливает не только возможность его приспособления как биологического существа к условиям внешней среды, что само по себе немаловажно, но и возникновение его социальных потребностей, возможность его социальной адаптации, развития личности, самореализации и самоутверждения. Информация является основным средством взаимодействия человека с другими людьми, без которого решение перечисленных задач не представляется возможным. Посредством информации осуществляется процесс воспитания, образования, с ее помощью происходит овладение трудовыми навыками, формируется представление человека о возможных способах удовлетворения нужд, потребностей и реализации интересов, осуществляются мотивация его деятельности, а также в определенной мере и сама деятельность.

Нанесение вреда информации, способности человека ее формировать, воспринимать и осмысливать чревато негативными последствиями для человека как социального и биологического существа, снижает возможность его выживания в реальном мире.

Информационная безопасность человека состоит в невозможности нанесения вреда ему как личности, социальная деятельность которой во многом базируется на осмыслении получаемой информации, информационных взаимодействиях с другими индивидами и которая часто использует информацию в качестве предмета деятельности.

Определенное ***«информационное измерение»*** присуще ***организациям***. Содержание их информационной безопасности заключается в защищенности, связанной с информацией и информационной инфраструктурой деятельности по достижению целей, а также «информационных» активов организации — информационных систем и ресурсов, объектов права интеллектуальной собственности, имущественных прав на эти объекты, личных неимущественных прав членов организации, прав на сохранение установленного режима доступа к сведениям, составляющим охраняемую законом тайну.

Эти составляющие объекта информационной безопасности и защищаются от внешних и внутренних угроз. В случае, когда руководство организации не видит необходимости в принятии мер по защите своих действий, например в связи с кажущейся незначительностью рисков, содержание информационной безопасности предприятия может быть сведено к защищенности конкретной информации, раскрытие которой может нанести заметный ущерб коммерческой деятельности. Подобную информацию обычно относят к коммерческой тайне.

Информационная безопасность общества заключается в невозможности нанесения вреда его духовной сфере, культурным ценностям, социальным регуляторам поведения людей, информационной инфраструктуре и передаваемым с ее помощью сообщениям.

«Информационное измерение» государства определяется информационным наполнением его деятельности. Деятельность государства, с содержательной точки зрения, заключается в выполнении функций государства, например, таких общесоциальных функций, как обеспечение безопасности, ликвидация последствий стихийных бедствий и экологических катастроф, реализация социальных программ поддержки здравоохранения, социального обеспечения нетрудоспособных, защита прав и свобод граждан.

«Информационное» наполнение деятельности государства определяется деятельностью его органов, с одной стороны, по стимулированию развития информационной инфраструктуры и активности информационной деятельности граждан, защите их прав и свобод в этой области, а с другой — по обеспечению законных ограничений на доступ к информации, несанкционированное раскрытие которой может нанести ущерб интересам личности, общества и государства.

Нанесение вреда деятельности органов государства способно существенно снизить его возможности выполнения государствен-

ных функций. Так, безнаказанное нарушение тайны переговоров, личной и семейной тайн подрывает доверие граждан к государству, уменьшает социальную поддержку процессов его функционирования; блокирование команд на боевое использование сил и средств ведения вооруженной борьбы лишает государство возможности отражения внешней агрессии; подделка таможенных деклараций лишает его возможности противостоять угрозам в экономической сфере жизнедеятельности общества.

Информационная безопасность государства заключается в невозможности нанесения вреда его деятельности по выполнению функций управления делами общества, связанных с использованием информации и информационной инфраструктуры общества.

Информационная коммуникация осуществляется посредством среды распространения информации, принимающей в современном обществе форму информационной инфраструктуры. Нанесение вреда этой инфраструктуре, передаваемым сообщениям и содержащимся в них сведениям может привести к нарушению информационной коммуникации и, как следствие, к разрушению целостности общества, дестабилизации деятельности его институтов и соответственно основ его существования.

Объектом обеспечения информационной безопасности в определенных случаях может выступать информационная система. Тогда под информационной безопасностью будет пониматься «защищенность информации и поддерживающей инфраструктуры от слу-

Рис. 6

чайных или преднамеренных воздействий естественного или искусственного характера, чреватых нанесением ущерба владельцам или пользователям информации и поддерживающей инфраструктуры»[1].

В наиболее общем виде ***информационная безопасность*** может быть определена как невозможность нанесения вреда свойствам объекта безопасности, обусловливаемым информацией и информационной инфраструктурой.

Структура данного понятия приведена на рис. 6.

На основе вышеизложенного можно сформулировать следующее определение рассматриваемого явления.

Обеспечение информационной безопасности характеризуется деятельностью по недопущению вреда свойствам объекта безопасности, обусловливаемым информацией и информационной инфраструктурой, а также средствами и субъектами этой деятельности.

Контрольные вопросы

1. Раскройте содержание объектов и субъектов безопасности, объектов и субъектов обеспечения информационной безопасности.
2. Приведите определения организации, юридического лица. Перечислите виды организаций, участвующих в гражданских отношениях.
3. Приведите определение государства. Перечислите его основные функции.
4. В чем заключается сущность информационной безопасности организаций и государства?

[1] *Бетелин В. Б., Галатенко В. И.* Информационная безопасность России. Опыт составления карты / Jet Info. — № 1, 1998. — С. 4—11.

Глава 4

СИСТЕМА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

4.1. Обеспечение информационной безопасности организации

При всем многообразии видов организаций, направлений и масштабов их деятельности, численности участников ***основными объектами обеспечения информационной безопасности***, как правило, являются:

– информация в форме сведений (сведения об участниках организации, о состоянии рынка и ее активов; репутация организации и доброе имя участников организации и т. п.);

– информация в форме сообщений (документы, закрепляющие права собственности организации на материальные и нематериальные активы; документация бухгалтерского учета, налоговые декларации, договоры на выполнение работ и оказание услуг; документация на выпускаемые изделия и т. п.);

– информационная инфраструктура (автоматизированные системы обработки информации и технологического управления; техническое и программное обеспечение информационных и коммуникационных систем и сетей связи, используемых в организации, и т. п.);

– правовой статус организации как субъекта информационной сферы (права на объекты интеллектуальной собственности, на выполнение работ и оказание услуг, на доступ к открытой информации государственных органов, на коммерческую тайну и т. п., а также обязанности по представлению в уполномоченные государственные органы сведений о результатах экономической деятельности, по соблюдению режима персональных данных, по представлению заинтересованным лицам документов в случае направления заявки на участие в конкурсах и аукционах и т. п.).

Наиболее опасные угрозы безопасности этих объектов проявляются в следующих формах:

– мошенничество, связанное с завладением чужим имуществом или приобретением права на него путем обмана или злоупотребления доверием, основанных на неправомерном доступе к информационно-коммуникационным системам, конфиденциальной информации, на подделке или искажении электронных документов в информационных и коммуникационных системах, сетях связи;

– клевета, основанная на распространении заведомо ложной информации, порочащей честь и достоинство руководителей организации;

– нарушение авторских и смежных прав, связанных с объектами интеллектуальной собственности;

– шантаж, связанный с угрозой распространения персональных данных, иной информации, охраняемой законом в режиме тайны;

– противоправное раскрытие информации ограниченного доступа третьим лицам;

– уничтожение или повреждение информационных ресурсов, информационно-коммуникационных систем и сетей связи посредством использования и распространения вредоносных программ, нарушения правил эксплуатации ЭВМ и их сетей;

– причинение имущественного ущерба собственнику или иному владельцу информационно-коммуникационных систем и сетей связи путем обмана или злоупотребления доверием без признаков хищения.

Вследствие проявления указанных угроз существенно возрастают риски, связанные с осуществлением основной деятельности организации (риск утраты репутации, риск ликвидности, операционные риски, риски утраты собственности или важных активов организации). Эти риски связаны с возможностью возникновения ситуаций проявления угроз, требующих дополнительных, часто существенных затрат материальных, людских, временных, финансовых и иных ресурсов на ликвидацию последствий проявления угроз. Увеличение рисков приводит к увеличению издержек и соответствующему снижению эффективности деятельности организации, уменьшению ее конкурентоспособности.

Система обеспечения информационной безопасности организации характеризуется двумя составляющими: деятельностью по подготовке и реализации мер, направленных на противодействие проявлению угроз информационной безопасности и минимизацию последствий этих проявлений; субъектами этой деятельности.

Деятельность по обеспечению информационной безопасности организаций базируется на следующих основных принципах:

– законность, заключающаяся в строгом и неуклонном исполнении норм законодательства Российской Федерации, соблюдении прав и свобод человека и гражданина;

– непрерывность, предполагающая рассмотрение деятельности в качестве одной из функций организации;

– комплексность, заключающаяся во всестороннем анализе факторов, оказывающих влияние на риски информационной безопасности, при планировании данной деятельности и использо-

вании всех имеющихся возможностей и выделенных ресурсов для реализации составленных планов;

– замкнутость, заключающаяся в совместном осуществлении деятельности по предупреждению проявления угроз, снижению их опасности, выявлению проявлений угроз, минимизации последствий этих проявлений, а также по оценке эффективности выполнения планов противодействия угрозам и их соответствующего уточнения.

В этой деятельности широко используются методы поощрения, убеждения и принуждения.

Меры по противодействию проявлению угроз информационной безопасности организации и минимизации последствий этих проявлений охватывают три основных направления деятельности:

– управление персоналом;

– организация объектового режима;

– организационно-техническое обеспечение.

Меры по управлению персоналом направлены на минимизацию рисков, связанных с проявлением личностных свойств и качеств участников организации, а также взаимодействующих с ней субъектов. Они включают подбор и расстановку кадров, обеспечение должной мотивации сотрудников к добросовестной работе, подготовку и повышение их квалификации.

Меры по организации объектового режима нацелены на минимизацию рисков, связанных с возможными попытками нанесения ущерба организации ее участникам и взаимодействующим с ней субъектам. Эти мероприятия включают осуществление пропускного и внутриобъектового режимов, в том числе установление и поддержание режимов информации, информационно-коммуникационных систем и систем связи, контроль поддержания установленных режимов и проведение служебных расследований по фактам их нарушения. При этом режимы информационно-коммуникационных систем и систем связи направлены на достижение требуемых значений основных свойств безопасности используемых в организации информационных технологий: конфиденциальности, целостности и готовности к использованию.

Меры по организационно-техническому обеспечению позволяют использовать возможности техники для установления и поддержания объектового режима. Они включают мероприятия по использованию средств защиты информации, информационных и коммуникационных систем, средств связи, а также по установлению и реализации политики безопасности в информационно-коммуникационных системах.

Важную роль в эффективной реализации мер по противодействию угрозам информационной безопасности играет нормативно-методическое обеспечение.

Основными *субъектами обеспечения информационной безопасности организаций* являются создаваемые в них координационные (например, советы по безопасности информационных технологий) и кадровые органы, специализированные структурные подразделения по вопросам информационной безопасности или должностные лица, а также структурные образования, специализирующиеся на оказании услуг в данной области, объединяемые в единую систему.

Структура указанной системы и ее составных частей может быть различной. Например, в организации может быть создан совет по безопасности информационных технологий, который решает вопросы выработки внутренней политики в этой области, ее реализации и нормативно-методического обеспечения.

Для качественного выполнения данных функций в состав совета включают представителей высшего руководства организации и должностных лиц, осуществляющих непосредственное управление обеспечением информационной безопасности. В некоторых случаях управление этой деятельностью может быть возложено на ответственных сотрудников соответствующих структурных подразделений.

4.2. Обеспечение информационной безопасности Российской Федерации

Осуществление деятельности по обеспечению информационной безопасности Российской Федерации возложено на государство, которое в соответствии с законодательством является основным субъектом обеспечения безопасности.

Под *информационной безопасностью Российской Федерации* понимается состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства.

В соответствии с Доктриной информационной безопасности Российской Федерации *национальные интересы в информационной сфере* включают следующие основные составляющие:

– соблюдение конституционных прав и свобод человека и гражданина в области получения информации и пользования ею, обеспечение духовного обновления России, сохранение и укрепление нравственных ценностей общества, традиций патриотизма и гуманизма, культурного и научного потенциала страны;

– информационное обеспечение государственной политики Российской Федерации;

– развитие современных информационных технологий, отечественной индустрии информации, обеспечение потребностей внутреннего рынка ее продукцией и выход этой продукции на мировой рынок; обеспечение накопления, сохранности и эф-

фективного использования отечественных информационных ресурсов;

– защита национальных информационных ресурсов от несанкционированного доступа, обеспечение безопасности информационных и телекоммуникационных систем.

Основными объектами обеспечения информационной безопасности Российской Федерации являются ее национальные интересы:

– информация в форме сведений (свобода мысли, национальные культурные ценности);

– информация в форме сообщений (архивные документы; документы, являющиеся музейными предметами или составляющие музейные коллекции; тиражированные документы);

– информационная инфраструктура (сети связи и инфраструктура информатизации; инфраструктура средств массовой информации и книгоиздания; инфраструктура открытых информационных ресурсов библиотек, архивных и музейных фондов);

– правовой статус субъектов информационной сферы Российской Федерации (совокупность реальных прав и обязанностей субъектов).

К ***угрозам информационной безопасности Российской Федерации***, в частности, относятся:

– противодействие реализации гражданами своих конституционных прав на личную и семейную тайну, тайну переписки, телефонных переговоров и иных сообщений;

– противоправные сбор и использование информации;

– разработка и распространение программ, нарушающих нормальное функционирование информационных и информационно-телекоммуникационных систем, в том числе систем защиты информации;

– уничтожение, повреждение, радиоэлектронное подавление или разрушение средств и систем обработки информации, телекоммуникации и связи;

– утечка информации по техническим каналам;

– внедрение электронных устройств для перехвата информации в технические средства обработки, хранения и передачи информации по каналам связи, а также в служебные помещения органов государственной власти, предприятий, учреждений и организаций независимо от формы собственности;

– уничтожение, повреждение, разрушение или хищение машинных и других носителей информации;

– перехват информации в сетях передачи данных и на линиях связи, дешифрование этой информации и навязывание ложной информации;

– использование несертифицированных отечественных и зарубежных информационных технологий, средств защиты информации, средств информатизации, телекоммуникации и связи при

создании и развитии российской информационной инфраструктуры;

– несанкционированный доступ к информации, находящейся в банках и базах данных;

– нарушение законных ограничений на распространение информации.

Деятельность по обеспечению информационной безопасности Российской Федерации осуществляется на основе принципов, разделяемых на общие и особенные.

К наиболее важным *общим принципам* деятельности по обеспечению безопасности относятся гуманизм, конкретность, эффективность, сочетание гласности и профессиональной тайны[1], законность и конституционность[2].

Принцип гуманизма заключается в обеспечении прав и свобод человека и гражданина при осуществлении противодействия угрозам информационной безопасности, недопущении противоправных посягательств на его личность, унижения чести и достоинства человека, произвольного вмешательства в его частную жизнь, личную и семейную тайны, ограничения свободы его информационной деятельности, а также в минимизации ущерба этим правам и свободам в случаях, когда их ограничение осуществляется на законных основаниях.

Принцип конкретности состоит в обеспечении безопасности применительно к конкретным жизненным обстоятельствам с учетом разнообразных форм проявления объективных законов на основе достоверной информации как о внутренних и внешних угрозах, так и о возможностях противодействия им. Достоверная информация позволяет установить конкретные формы проявления угроз, определить в соответствии с этим цели и действия по обеспечению безопасности, конкретизировать методы противодействия угрозам, а также необходимые для их реализации силы и средства.

Принцип эффективности заключается в достижении целей противодействия при наименьших затратах сил и средств. Обеспечение информационной безопасности в любой социальной общности требует определенных материальных, финансовых и людских ресурсов. Исходя из этого обеспечение безопасности, как и всякая общественно полезная деятельность людей, должно осуществляться рационально и эффективно. Обычно критерием эффективности, который применяется на практике, является отношение размера предотвращенного ущерба от реализации угроз к затратам на противодействие этим угрозам.

---

[1] *Гыскэ А. В.* Теоретико-методологические аспекты обеспечения общественной безопасности Российской Федерации. — М.: Прогрессивные биомедицинские технологии, 2000. — С. 41.

[2] Теория государства и права. — Т. 1. — С. 171.

Принцип сочетания гласности и профессиональной тайны состоит в нахождении и поддержании необходимого баланса между открытостью деятельности по противодействию угрозам информационной безопасности, позволяющей добиться доверия и поддержки общества, и защитой определенной информации, разглашение которой может снизить эффективность противодействия угрозам безопасности.

Принцип законности и конституционности означает осуществление всех свойственных государственным организациям и должностным лицам функций в строгом соответствии с действующей конституцией, законами и подзаконными актами, согласно установленной в законодательном порядке компетенции. Строгое и неуклонное соблюдение законности и конституционности должно быть непременным требованием, принципом деятельности не только государственных, но и негосударственных органов, учреждений и организаций.

К числу особенных принципов деятельности по обеспечению информационной безопасности следует отнести прежде всего глобальность.

Принцип глобальности заключается в том, что указанная деятельность должна осуществляться согласованно как в конкретном обществе, так и в международном сообществе. К важным формам осуществления деятельности по обеспечению информационной безопасности относится социальное регулирование, в том числе правовые и организационные мероприятия.

Важнейшими формами осуществления деятельности по обеспечению информационной безопасности являются регулятивная и организационная формы.

Регулятивная форма деятельности по обеспечению информационной безопасности характеризуется нормами регулирования общественных отношений по поводу противодействия угрозам и мерами по выработке и поддержанию этих норм. Выделяют два основных типа норм: технические и социальные.

• *Технические нормы* определяют порядок взаимодействия человека с окружающей средой, осуществления деятельности по созданию материальных благ, пользования орудиями труда, в частности средствами и системами информатизации, телекоммуникации и связи. Современную систему технических норм составляют правила использования современных информационных технологий, правила защиты информации и информационных систем от несанкционированного доступа, правила пользования средствами автоматизации управления и обработки информации. Следование этим правилам способствует более производительной и эффективной работе, предупреждает нанесение ущерба таким объектам национальных интересов, как информация и информационно-телекоммуникационные системы, производственный травматизм и заболевания.

• *Социальные нормы* регулируют поведение индивидов и подразделяются на поддерживаемые силами социальной общности без участия государства и на поддерживаемые с использованием государственного принуждения.

Первые включают прежде всего мораль, обычаи и традиции, корпоративные и религиозные нормы. Эти нормы играют большую роль в противодействии угрозам сохранения национальной идентичности.

• *Мораль, или моральные нормы,* — правила поведения, основанные на представлениях национальной общности о добре и зле, справедливости и несправедливости, честности и бесчестии и других подобных этических качествах. Значительная часть моральных норм вырабатывается и поддерживается нацией в целом или большей частью ее социальных групп.

Под *обычаями* понимаются правила поведения, сложившиеся в далеком прошлом и поддерживаемые в силу привычки в современном обществе. Норма, ставшая обычаем, оказывает свое регулирующее воздействие в силу ее эмоционального восприятия членами общества, привыкшими к ее соблюдению настолько, что реализация данной нормы превратилась в потребность.

Традиции представляют собой правила поведения, которые определяют порядок, процедуру проведения каких-либо мероприятий, связанных с торжественными или знаменательными, значительными событиями в жизни индивида как представителя конкретной нации, а также другие элементы социального и культурного наследия, передающиеся от поколения к поколению (идеи, взгляды, вкусы, образ действия и мысли и т.п.).

Широкое распространение в современном обществе получили нормы общественных объединений, политических партий, закрепленные их уставами, — *корпоративные нормы.* Эти нормы определяют порядок участия членов в деятельности конкретных организаций, их взаимоотношения с руководством, взаимодействие с другими организациями.

Религиозные нормы представляют собой правила, установленные различными вероисповеданиями. Такие нормы содержатся в Библии, Коране, Талмуде и других религиозных книгах либо в сознании верующих, исповедующих языческие, многобожеские культы. Они определяют порядок совершения религиозных обрядов.

Общим для всех этих норм является то, что они, как правило, составляют значительную часть национальных духовных ценностей, отличающих одну нацию от другой.

Важной составляющей социального регулирования деятельности по обеспечению информационной безопасности является ***правовое регулирование общественных отношений.*** Оно заключается в установлении определенных правовых норм осуществления наибо-

лее важных общественных отношений и охраны этих норм от нарушения с использованием государственного принуждения. Правовое регулирование отношений в целях обеспечения информационной безопасности осуществляется в рамках правовой деятельности государства, в структуре которой выделяются законодательная (правотворческая), правоприменительная и судебная деятельность.

Законодательная деятельность заключается в подготовке, принятии и издании законодательными органами нормативных правовых актов, регулирующих отношения в области удовлетворения национальных интересов в информационной сфере, а также создающих условия для предотвращения реализации угроз информационной безопасности или минимизации их воздействия на защищаемые общественные отношения. Законодательная деятельность направлена на создание правовой основы выполнения государственными органами задач по противодействию угрозам, на установление таких правил реализации общественных отношений в рассматриваемой области, при которых ни внешние, ни внутренние угрозы не оказывают на защищаемые отношения существенного негативного воздействия. Совокупность нормативных правовых актов, являющихся источниками права в данной сфере, составляют основу так называемого нормативного правового обеспечения информационной безопасности.

Правоприменительная деятельность представляет собой основанную на законодательстве оперативную, повседневную реализацию органами исполнительной власти (государственного управления) функций государства в области обеспечения информационной безопасности. Эта деятельность осуществляется в следующих формах:

– подготовка, принятие и исполнение решений органов исполнительной власти об осуществлении конкретных мероприятий по противодействию угрозам информационной безопасности;

– координация деятельности органов исполнительной власти в процессе подготовки и реализации конкретных мероприятий;

– осуществление правоприменительной практики в рассматриваемой области;

– проведение консультативной и информационной деятельности органов исполнительной власти, направленной на создание условий для эффективного выполнения возложенных на эти органы задач;

– выполнение учетной, аналитической, прогнозной и программной работы, административных договоров;

– взаимодействие органов исполнительной власти с другими ветвями и институтами государственной власти в целях согласования усилий по противодействию угрозам;

– информационное обеспечение всех субъектов противодействия угрозам информационной безопасности в системе исполнительной власти;

– государственный контроль за законностью деятельности субъектов правового регулирования в рассматриваемой области[1].

Судебная деятельность охватывает реализацию функции государства по обеспечению правосудия в процессе выполнения задач противодействия угрозам информационной безопасности. Эта деятельность является неотъемлемой составляющей обеспечения информационной безопасности, так как позволяет каждому реализовать свое конституционное право на объективное рассмотрение всех обстоятельств, связанных с применением к нему мер государственного принуждения.

Правовое обеспечение информационной безопасности характеризуется двумя основными составляющими: деятельностью государства по обеспечению информационной безопасности, осуществляемой в правовой форме; органами государственной власти, осуществляющими эту деятельность. Данное правовое обеспечение возникает в процессе взаимодействия права (как средства регулирования общественных отношений) и государства (как основного субъекта противодействия угрозам его безопасности). Правовое обеспечение проявляется в воздействии правовых механизмов на общественные отношения в целях осуществления функций государства по противодействию угрозам безопасности.

Правовое обеспечение информационной безопасности регулирует отношения в области организации противодействия угрозам информационной безопасности как отдельных организаций, так и Российской Федерации в целом, во многом определяя структуру и принципы других видов обеспечения информационной безопасности, в частности организационного обеспечения.

Правовые средства обеспечения информационной безопасности выражаются в установлениях (субъективные права, обязанности, льготы, запреты, поощрения, наказания и т.п.) и деяниях (технологии — акты реализации прав и обязанностей)[2], противодействующих реализуемым в информационной сфере угрозам интересам субъектов права и обеспечивающих достижение социально полезных целей. Они отражают функциональную, прикладную сторону правовой системы, выступают в качестве элементов механизма правового регулирования, во многом определяя эффективность данного механизма.

Организационное обеспечение информационной безопасности состоит в осуществлении планирования и управления материальными, людскими, финансовыми и другими ресурсами государства, выделяемыми для противодействия угрозам. В рамках этой деятельности могут приниматься меры, направленные на разви-

[1] Исполнительная власть в Российской Федерации. Проблемы развития / отв. ред. И.Л.Бачило. — М.: Юрист, 1998. — С. 206.

[2] *Малько А.В.* Проблемы правовых средств. В кн.: Проблемы теории государства и права. — М.: Проспект, 1999. — С. 326.

тие научных исследований в области повышения устойчивости информационной инфраструктуры к проявлению угроз, на содействие в установленном законодательством порядке работе общественных организаций, ставящих своей целью противодействие угрозам информационной безопасности и определение форм возможного взаимодействия с ними, на согласование деятельности федеральных органов исполнительной власти и органов исполнительной власти субъектов Российской Федерации в области противодействия угрозам, на развитие системы массовой информации, способной удовлетворять потребности граждан в актуальных, достоверных сведениях об интересующих их событиях общественной жизни, обеспечивать их своевременное поступление к гражданам и т.д.

Организационное обеспечение информационной безопасности Российской Федерации осуществляется с использованием ***средств технического, кадрового, материального, финансового, информационного и научного обеспечения***.

Средства технического обеспечения информационной безопасности образуются совокупностью технических и программных средств защиты информации, предотвращения несанкционированного доступа в информационные, телекоммуникационные и вычислительные системы и сети связи, а также методического обеспечения их использования.

Средства кадрового обеспечения информационной безопасности характеризуются программами подготовки кадров по различным аспектам данной деятельности, а также используемыми учебными и методическими материалами.

Средства материального обеспечения характеризуются совокупностью объектов, выделяемых для размещения средств технологического обеспечения, сил, участвующих в обеспечении информационной безопасности, средств организации их деятельности и т.п.

Средства финансового обеспечения представляют собой совокупность экономических инструментов получения, привлечения, перераспределения и использования денежных средств для решения задач обеспечения информационной безопасности.

Средства информационного обеспечения образуются совокупностью информационных фондов и банков данных, используемых в процессе решения задач обеспечения информационной безопасности, а также средств их актуализации.

Средства научного обеспечения информационной безопасности определяются совокупностью научных теорий, концепций, категорий, закономерностей и методов, предназначенных для изучения процессов и явлений развития информационной сферы общества, угроз национальным интересам, реализуемым в этой сфере, и для противодействия этим угрозам.

Рис. 7

Общая структура средств обеспечения информационной безопасности представлена на рис. 7.

Основные субъекты обеспечения информационной безопасности Российской Федерации объединены в рамках государственной системы защиты информации. К их числу относятся:

– службы контроля, надзора и обеспечения информационной безопасности государственных органов;

– специализированные предприятия и организации, осуществляющие деятельность в области разработки средств и предоставления услуг по защите информации;

– сертификационно-испытательные центры; аттестационные центры;

– службы безопасности и защиты информации предприятий и организаций, осуществляющих обработку персональных данных, конфиденциальной информации и информации, составляющей государственную тайну.

Контрольные вопросы

1. Раскройте содержание обеспечения информационной безопасности организации.

2. Перечислите наиболее важные объекты информационной безопасности организации и угрозы безопасности этих объектов.

3. Опишите структуру системы обеспечения информационной безопасности организации.

4. Раскройте содержание информационной безопасности Российской Федерации.

5. Перечислите наиболее важные объекты информационной безопасности Российской Федерации и основные угрозы их безопасности.

6. Перечислите принципы обеспечения информационной безопасности Российской Федерации и раскройте их содержание.

7. Перечислите основные виды обеспечения информационной безопасности и раскройте их содержание.

ЧАСТЬ II
ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Глава 5
ЭЛЕМЕНТЫ ТЕОРИИ ПРАВА

5.1. Понятие «право». Субъективное, объективное (позитивное) и естественное право

Термином «право» обозначается обоснованная, оправданная свобода или возможность поведения человека в его взаимоотношениях с другими людьми, которая признана и поддерживается обществом.

В зависимости от формы проявления общественного признания этой свободы и способа ее поддержки со стороны общества различают следующие виды права:

обычное право — свобода, или возможность поведения, основанная на обычаях, т.е. нормах поведения, вошедших в привычку (обычай старшинства, первенства в очереди);

моральное право — свобода, или возможность поведения, основанная на принципах добра, справедливости (заботливое отношение детей к родителям, уважение к женщине);

корпоративное право — свобода, или возможность поведения, основанная на уставных и иных положениях, которые действуют внутри общественных, негосударственных объединений, организаций, партий (право избирать и быть избранным в руководящие органы, право руководящих органов налагать взыскания);

естественное право — свобода, или возможность поведения, непосредственно вытекающая из опыта жизни человечества, из разума, во многом определяющая мораль и обычаи (право на жизнь, право на свободу, право на равный эквивалент при товарном обмене);

юридическое право — свобода, или возможность поведения, основанная на законе, иных официальных источниках права.

В дальнейшем термин «право» будет использоваться прежде всего в юридическом смысле.

Юридическое право представляет собой систему общеобязательных норм, выраженных в законах, иных признаваемых государством источниках права и являющихся общеобязательным осно-

ванием для определения правомерно-дозволенного, запрещенного и предписанного поведения.

Право применительно к конкретному человеку (субъекту) обозначается термином ***«субъективное право»*** и означает свободу, или возможность его юридически обеспеченного поведения, т.е. поведения, которое поддерживается государственным принуждением. Субъективному праву одного человека соответствуют субъективные обязанности других людей, которые совместно и создают пространство субъективной свободы.

Правом регулируется поведение не только отдельных граждан, но и организаций, государственных органов. Система норм, правил поведения, выраженных в законах и устанавливающих правомерное и неправомерное поведение граждан, организаций и государства, обозначается термином ***«объективное (позитивное) право»***. Как институт общества позитивное право предназначено для официального определения меры дозволенного и недозволенного поведения людей, юридически обоснованной свободы их действий. Как явление общественной жизни позитивное право создает условия для решения конкретных жизненных ситуаций на твердом публичном основании, утверждает с помощью власти принципы и правила взаимодействия людей.

В настоящее время в развитых странах позитивное право в определенной мере базируется на *естественном праве*, закрепляя наиболее важные его положения и создавая таким образом государственные гарантии их применения в обществе. Более того, нормы естественного права часто используются в качестве критерия соответствия норм позитивного права основному назначению права — поддержанию справедливости в обществе.

Необходимость такого сравнения обусловлена различиями в происхождении и направленности норм естественного и позитивного права.

Так, нормы естественного права вырабатываются в ходе всей жизни человечества и определяют прежде всего правила поведения, являющиеся критически важными для выживания общества в реальных условиях его существования. Они, с одной стороны, составляют существо знаний в области социального взаимодействия, знаний, которые человечество приобрело за свою длительную историю, а с другой — являются критериями поощряемого обществом справедливого поведения.

Нормы позитивного права специально создаются людьми для регулирования социально важных сторон общественной жизни. Учитывая, что эти нормы властно утверждаются в общественной жизни в качестве постоянного, непререкаемого критерия для обязательного поведения, обеспечения их социальной справедливости, представляется важной их согласованность с основными нормами естественного права.

Позитивное право как совокупность закрепленных в законах, других законодательных актах норм поведения наполняется реальной жизнью в процессе использования людьми субъективных прав и выполнения возложенных на них обязанностей, а также правоприменительной деятельности органов исполнительной власти и отправления правосудия. Правосудие является ключевым фактором развития и жизни права. Оно предназначено для разрешения с позиции права и на основе публичной власти спорных конфликтных ситуаций, возникающих вследствие столкновения интересов различных субъектов общественной жизни или иных причин.

5.2. Формы и признаки позитивного права. Публичное и частное право

Позитивное право может существовать в четырех основных формах: обычного права, религиозного права, права судей и права законодателя.

В форме ***обычного права*** юридические нормы возникают на основе обычаев, которые в результате длительного действия стали привычкой, непререкаемым примером поведения. Обычаи, обосновывающие и оправдывающие поведение людей, получают в ряде случаев юридическое признание и рассматриваются в качестве достаточного критерия правомерного поведения. Этим обычаям государство придает общеобязательное значение и их соблюдение гарантирует своей силой.

В форме ***религиозного права*** юридические нормы возникают на основе положений религиозных текстов, которые почитаются в качестве священных. В этой форме права положениям религиозных текстов, определяющих правила поведения людей, государство придает общеобязательную силу юридических норм.

В форме ***права судей*** юридические нормы возникают в результате судебного решения. Часто судебные решения, которые приняты по вопросу, не урегулированному обычаем или законодательным актом, становятся прецедентом для разрешения подобных жизненных ситуаций в будущем и таким образом приобретают свойства нормы.

В форме ***права законодателя*** нормы позитивного права формируются в процессе деятельности уполномоченных государственных органов или должностных лиц. Обычно такими полномочиями наделяются высшие, представительные органы государственной власти. Результатом их деятельности становятся нормативные правовые акты, закрепляющие новые юридические нормы, а также положения, отменяющие или изменяющие уже действующие нормы.

В единстве с другими активными элементами правовой действительности — правовой идеологией (т.е. активной частью

правосознания, непосредственно влияющей на законодательство и юридическую практику) и судебной (юридической) практикой — позитивное право образует правовую систему жизни общества.

Наиболее известными в настоящее время ***правовыми системами*** являются:

романо-германская, основанная на праве законодателя (континентальная Европа);

прецедентная, основанная на праве судей (Великобритания и США);

религиозная, базирующаяся на священной для мусульман книге — Коране (мусульманское право характерно, например, для Ирана).

Данные правовые системы различаются прежде всего источниками права — исходящими от государства или признанными им официально-документальными формами выражения и закрепления норм права, придания им юридического, общеобязательного значения.

Позитивное право обладает рядом ***признаков***, из которых наиболее существенны следующие:

– общеобязательная нормативность — нормы права распространяют свое действие на всю территорию и на ее население;

– выражение норм в законах, иных признаваемых государством источниках права;

– действие через дозволения, через субъективные права, очерчивающие сферу юридически дозволенного поведения, сферу свободы личности, ее автономности;

– государственная обеспеченность — нормы права имеют поддержку государства как мощной социальной силы, способной в установленных правом случаях и форме гарантированно обеспечить наступление ожидаемых от юридических норм результатов.

Различают две взаимосвязанные составляющие (стороны) позитивного права: публично-правовую и частно-правовую.

Публично-правовая сторона права отражает его свойства как инструмента деятельности государственной власти. С этой стороны право представляет собой социальное образование, базирующееся в основном на законах государственной власти. Оно легализует государственное насилие, делает акцент на запретах, обязанностях людей перед государством, а также на обязанностях государства перед людьми.

Государство как политико-территориальная суверенная организация публичной власти располагает специальным аппаратом и способно делать свои веления обязательными для населения территории, на которую распространяется его власть. Важно отметить, что государство и право находятся в определенной взаимо-

связи. Право закрепляет основы существования государства и придает ему легитимность в глазах населения, а государство создает условия для формирования и существования права.

Частно-правовая сторона права отражает его свойства как средства осуществления государственных гарантий свободы человека, его экономической и духовной самостоятельности, защиты достоинства его личности. С этой стороны государство выступает в качестве основного условия свободы человека, его независимости.

Каждая из этих составляющих развивается в составе относительно самостоятельных сфер — публичного и частного права соответственно.

Публичное право — область «государственных дел», т.е. само устройство и деятельность государства как публичной власти, деятельность всех публичных институтов, регулирование деятельности аппарата государства, административные отношения, государственная служба, уголовное преследование и ответственность; словом, — это правовые институты, построенные на началах власти и подчинения, на отношениях субординации.

Частное (гражданское) право — область «частных» дел, т.е. правового статуса личности, частной собственности, договорных отношений, наследования, интеллектуальной собственности; ина-

Рис. 8

че говоря, — это правовые институты, построенные на началах автономии, юридического равенства субъектов, их несоподчиненности между собой.

Общая структура права схематично представлена на рис. 8.

5.3. Нормы права, правоотношения, субъекты и объекты права, юридические факты

Воздействие права на поведение людей в общественных отношениях осуществляется посредством механизма правового регулирования, образуемого упорядоченной совокупностью используемых для этого правовых средств. Основными звеньями этого механизма являются юридические нормы, правовые отношения (правоотношения), акты реализации прав и обязанностей, а также акты применения права.

Действие правового механизма позволяет на строго логической основе найти прямые ответы на реальные жизненные ситуации, определяя, насколько правомерно, допустимо или недопустимо вел себя человек в конкретной ситуации, а также определяя в случае виновного или невиновного нарушения норм поведения справедливую меру юридической ответственности, которая может или должна быть применена к человеку, и способ применения этой ответственности.

Ключевым средством в правовом механизме является ***юридическая норма*** — общеобязательное правило поведения, выраженное в законах, иных признаваемых государством источниках права и выступающее в качестве критерия правомерно-дозволенного, запрещенного или предписанного поведения субъектов права.

Для норм права как правил поведения общего характера свойственны следующие принципиальные особенности:

– системность, отражающая свойство норм существовать и действовать не поодиночке, не каждая сама по себе, а в комплексе, в составе целых правовых институтов и более обширных подразделений права — отраслей;

– специализация, отражающая свойство норм закреплять какую-то одну, определенную юридическую операцию — установление общих положений (нормы — принципы), запрет (запрещающие нормы), применение принудительных мер в случае совершения правонарушения (правоохранительные нормы) и т.п.

По общей направленности действия правовые нормы подразделяются:

– на *регулятивные*, определяющие субъективные права и юридические обязанности субъектов, условия их возникновения и действия;

– *правоохранительные*, определяющие условия применения к субъекту мер государственно-принудительного воздействия, характер и содержание этих мер.

По способу воздействия на общественные отношения нормы подразделяются:

– на *управомочивающие*, предоставляющие субъекту право с положительным содержанием, т.е. право на совершение им тех или иных действий (например, распоряжаться имуществом, подавать иск в суд, получать пенсию);

– *запрещающие*, устанавливающие обязанность субъекта воздерживаться от совершения действий определенного рода (например, не совершать краж, не нарушать правила дорожного движения);

– *обязывающие*, возлагающие на субъекта обязанность совершать действия определенного содержания (например, платить налоги, регистрировать акты гражданского состояния).

По характеру воздействия на регулируемые общественные отношения нормы подразделяются на две категории:

– *императивные*, содержащие предписания, действующие независимо от усмотрения субъекта права;

– *диспозитивные*, содержащие предписания, выполнение которых необходимо в случае, если субъекты права не договорились об ином (порядок разрешения ситуации, связанной с гибелью предмета залога).

В структуре ***правовой нормы*** выделяются следующие элементы: гипотеза, диспозиция и санкция.

Гипотеза указывает на условия, при которых у субъектов права возникают права и обязанности, *диспозиция* — на содержание этих прав и обязанностей, а *санкция* — на неблагоприятные последствия, наступающие при нарушении нормы.

При анализе структуры правовых норм необходимо учитывать их специализацию, в результате которой в регулятивных нормах, как правило, имеются только гипотеза и диспозиция, а в правоохранительных — диспозиция и санкция.

Действие права проявляется в конкретных ***правоотношениях***, представляющих собой обусловленное правовой нормой отношение между субъектами, которые имеют субъективные права и юридические обязанности.

В наиболее общем случае правоотношения, как и правовые нормы, подразделяются на *регулятивные* — возникающие в процессе реализации субъективных прав, и *охранительные* — возникающие в связи с нарушением установленных правом норм проведения.

В структуру правоотношения входят: субъективные права и юридические обязанности, определяющие содержание правоот-

ношения; субъекты — носители права и обязанностей; объекты права.

Субъективные права определяют возможность субъекта права действовать дозволенным образом и требовать определенного поведения от других субъектов (лиц) в связи с реализацией данного права.

Основным средством обеспечения государством субъективных прав является возложение на другое лицо *юридических обязанностей* — предписанной субъекту меры должного, необходимого поведения. Юридические обязанности однозначны по их содержанию, императивны, непререкаемы, обеспечены юридическими механизмами, а также правом требования со стороны другого лица исполнения обязанности (право притязания).

Субъектами права являются лица (граждане, организации, общественные образования, государственные органы, учреждения и т.д.), обладающие правосубъектностью, т.е. способностью быть носителями прав и обязанностей, участвовать в правовых отношениях. *Правосубъектность* определяется двумя элементами: правоспособностью — способностью обладать субъективными правами и нести юридические обязанности; дееспособностью — способностью самостоятельно, своими действиями приобретать и осуществлять права, создавать для себя обязанности и исполнять их.

Основными *субъектами публичного права* являются индивидуальные субъекты (граждане, иностранные граждане, лица без гражданства), организации (коммерческие и некоммерческие организации, предприятия, государственные учреждения и т.п.), государство, государственные и муниципальные образования. Эти субъекты связаны между собой отношениями юридической субординации и подчиненности.

Основными *субъектами частного (гражданского) права* являются лица (физические и юридические), обладающие свойством формального юридического равенства независимо от того, в каких отношениях они находятся с точки зрения публичного права.

В гражданском праве *юридическим лицом* признается организация, которая имеет в собственности, хозяйственном ведении или оперативном управлении обособленное имущество и отвечает по своим обязательствам этим имуществом, а также может от своего имени приобретать и осуществлять имущественные и личные неимущественные права, нести обязанности, быть истцом и ответчиком в суде.

Особая разновидность юридических лиц — *унитарные (государственные* и *муниципальные) предприятия*, под которыми признаются коммерческие организации, не наделенные правом собственности на закрепленное за ними собственником имущество. Иму-

щество унитарного предприятия является неделимым и находится в государственной или муниципальной собственности.

Объект права — тот предмет окружающего мира, материальное или нематериальное благо, по поводу которого сложилось *правоотношение.*

Правоотношение отражает связь между субъектами права, которая возникает, изменяется или прекращается при наличии необходимых для этого ***юридических фактов*** — обстоятельств, с которыми нормы права связывают возникновение, изменение и прекращение правоотношений. Юридическими фактами являются, например, договор, акт назначения на должность, регистрация брака.

Нередко возникновение, изменение или прекращение правоотношения порождают не один какой-либо факт, а их совокупность.

Например, для возникновения правоотношения, связанного с назначением пенсии, нужны, по крайней мере, три факта — возраст, стаж и акт о назначении пенсии. Такая совокупность фактов называется *фактическим составом.*

По волевому признаку юридические факты подразделяют:

– на *события* — факты, возникающие независимо от воли людей (рождение человека, стихийное бедствие);

– *действия* — факты, порождаемые по воле людей (договоры, правонарушения).

Одной из важных разновидностью правоотношений являются ***правонарушения.***

Для возникновения отношения правонарушения необходимы, как правило, определенные юридические факты, образующие состав правонарушения:

– *объект* — нарушенное материальное или нематериальное благо;

– *субъект* — дееспособное лицо, совершившее правонарушение, т.е. нарушившее предписание, закрепленное в норме права;

– *объективная сторона* — само противоправное деяние, наступивший вредоносный результат и причинная связь между деянием и результатом;

– *субъективная сторона* — вина, т.е. отношение правонарушителя к деянию и его результату в форме умысла или неосторожности.

Возникновение отношения правонарушения в соответствии с законом приводит к возникновению правоотношений, связанных с применением юридической ответственности.

Юридическая ответственность — это применение к виновному лицу мер государственного принуждения за совершенное правонарушение. При применении юридической ответственности правонарушитель претерпевает меры государственного при-

нуждения за свою вину и поэтому несет определенные лишения, урон.

Юридическая ответственность отражает меру общественного осуждения правонарушителя, социальной опасности его поведения.

Для обеспечения устойчивости общественного развития крайне важным является реальное воплощение содержания юридических норм (***реализация права***) в фактическом поведении людей, в деятельности организаций и государственных органов.

Выделяют четыре основных вида реализации права:

– *использование* — субъект использует возможности, предоставляемые ему юридической нормой;

– *соблюдение* — субъект соблюдает установленные запреты;

– *исполнение* — субъект совершает активные действия во исполнение наложенных на него обязанностей;

– *применение* — властно-организационная деятельность компетентных органов и лиц, обеспечивающих в конкретных жизненных случаях реализацию юридических норм.

5.4. Источники права

Источником права называется официальный документ, созданный в соответствии с установленной процедурой и опубликованный уполномоченными государственными органами, а также содержащий нормы права или их элементы, правовые обычаи и судебные решения.

Источники права подразделяются на следующие группы:

– *общепринятые принципы и нормы международного права, международные договоры Российской Федерации*, являющиеся составной частью правовой система России;

– *законы* — юридические акты, обладающие высшей юридической силой на территории их действия по сравнению с другими национальными нормативными правовыми актами;

– *подзаконные акты*, принимаемые органами исполнительной власти во исполнение законов в пределах их компетенции.

Законы в Российской Федерации подразделяются на федеральные (конституционные и текущие) и законы субъектов Российской Федерации, принимаемые ими в пределах установленных Конституцией Российской Федерации предметов ведения.

Федеральные конституционные законы закрепляют основы общественного и государственного строя, конкретизируя и развивая положения Конституции.

Примерами таких законов являются федеральные законы «О Правительстве Российской Федерации» от 17 декабря 1997 г.

«О военном положении» от 30 января 2002 г. Текущие федеральные законы регулируют более частные отношения во всех сферах жизни общества — экономической, политической, культурной и др.

Законы субъектов Российской Федерации регулируют отношения, отнесенные к предметам ведения субъектов Российской Федерации.

Контрольные вопросы

1. В чем заключается содержание понятия «право» и каковы формы его проявления в общественной жизни?
2. В чем заключается содержание и какова структура позитивного права?
3. Что такое юридическая норма и какова ее структура?
4. В чем заключается различие между субъектами и объектами права?
5. В чем заключается юридическая ответственность?

Глава 6

ОСНОВЫ ТЕОРИИ ПРАВОВОГО ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

6.1. Содержание и структура правового обеспечения

Правовое обеспечение информационной безопасности является самостоятельным комплексным направлением правового регулирования отношений в области проявления угроз объектам информационной безопасности и противодействия этим угрозам на основе норм и институтов различных отраслей права (конституционного, гражданского, административного, уголовного и информационного).

Предмет правового обеспечения информационной безопасности представляет собой совокупность общественных отношений, на которые направлено правовое воздействие в целях недопущения, выявления и пресечения проявлений угроз объектам национальных интересов в информационной сфере, а также минимизации негативных последствий проявления этих угроз.

Общественные отношения, относящиеся к данному предмету, имеют следующие основные признаки:

– *принадлежность к регулируемым правом информационным отношениям*, т.е. общественным отношениям по поводу обладания необходимой информацией, передачи части имеющейся информации другим субъектам, а также сохранения в неизвестности оставшейся части информации;

– *принадлежность к объектам информационной безопасности*, которые представляются важными руководству организаций или государственных органов для эффективного достижения целей их деятельности;

– *обусловленность проявлением угроз* сохранности основных свойств объектов информационной безопасности организаций и государственных органов.

Совокупность норм и институтов права, регулирующих эти отношения, составляет содержание правового обеспечения информационной безопасности и может быть разделена по объектам безопасности на правовое обеспечение безопасности информации в форме сведений, правовое обеспечение безопасности информации в форме сообщений, правовое обеспечение безопасности информационной инфраструктуры и правовое обеспечение безопасности правового статуса субъекта информационной сферы.

Правовое обеспечение безопасности информации в форме сведений образуется совокупностью норм и институтов, регулирующих отношения по поводу следующих объектов: сведения, обладателем которых является субъект права; свобода мысли; субъективная значимость национальных культурных ценностей.

Цель противодействия заключается в предупреждении проявления угроз безопасности этих объектов и минимизации последствий проявления угроз.

Основная угроза сведениям, обладателем которых является субъект права, заключается в искажении этих сведений посредством навязывания ложной информации. В основу правового регулирования отношений в области противодействия навязыванию ложной информации положен принцип выделения социально опасных действий, связанных с передачей или распространением такой информации (клевета, обман и злоупотребление доверием, заведомо ложная реклама и т. п.), и их запрета под угрозой применения к виновным лицам административной или уголовной ответственности. Нормы права, регулирующие эти отношения, входят в состав отраслей административного или уголовного права.

Основная угроза свободе мысли заключается в применении средств нарушения независимости психической деятельности мозга человека, например, таких, как скрытые вставки, скрытая реклама.

Скрытая вставка представляет собой изображение, сюжет, мелодию или текстовое сообщение, которые являются составной частью программ, фильмов или компьютерных программ, относящихся к специальным средствам массовой информации. Они воспринимаются человеком через подсознание и (или) оказывают вредное воздействие на его здоровье.

В отличие от «скрытой вставки» дефиниция «скрытая реклама» в законодательстве определяется как реклама, которая оказывает не осознаваемое потребителем воздействие, в том числе путем использования специальных видеовставок (двойной звукозаписи) и иными способами[1].

Основу правовой конструкции регулирования отношений в рассматриваемых областях составляют нормы конституционного права, гарантирующие каждому человеку осуществление права на свободу мысли, а также нормы, предусматривающие возможность использования для защиты этого права целой системы юридических институтов, включающей институты конституционного контроля, судебной защиты, административно-правовой защиты, государственного надзора, международного контроля и международной судебной защиты[2]. Кроме того, в состав этой конструкции

---

[1] Федеральный закон «О рекламе» от 18 июля 1995 г. Ст. 9.

[2] Права человека / отв. ред. Е.А.Лукашева. — М.: НОРМА-ИНФРА М, 1999. — С. 459—530.

входят правовые нормы, закрепляющие конституционное право человека и гражданина на охрану здоровья и медицинскую помощь[1], в частности на восстановление психического здоровья человека, а также нормы, регулирующие отношения в области оказания ему необходимой медицинской помощи[2].

Основная угроза субъективной значимости национальных культурных ценностей заключается в их девальвации вследствие пропаганды образцов массовой культуры, основанных на культе насилия, а также духовных и нравственных ценностей, противоречащих принятым в российском обществе[3]. Эта угроза проявляется в виде деятельности граждан или их объединений по распространению идей религиозного экстремизма и нетерпимости, этнического превосходства или унижения. Распространение таких идей при отсутствии контрпропаганды со стороны общества и государства приводит к размыванию в индивидуальном и общественном сознании значимости традиционных ценностей, формированию представлений об отсутствии социальной поддержки этих ценностей.

Основу правового регулирования отношений в области противодействия этой угрозе составляет принцип закрепления в нормах права запрета на распространение и использование основных элементов культуры, основанной на идеях насилия, национальной и религиозной ненависти, оскорбляющих в связи с этим национальные культурные ценности российского народа, включая использование относящихся к ней символов, и юридической ответственности лиц и объединений граждан, нарушающих данный запрет.

Правовое обеспечение безопасности информации в форме сообщений определяется совокупностью правовых норм и институтов, регулирующих отношения, объектами которых являются сообщения, передаваемые по каналам связи, данные, накапливаемые и обрабатываемые в информационных системах, автоматизированных системах управления, а также документы как входящие, так и не входящие в информационные системы.

Основная цель правового регулирования в этой области состоит в предупреждении, выявлении и пресечении проявлений угроз безопасности этих объектов и минимизации последствий таких проявлений.

Основная угроза безопасности информации в форме сообщений заключается в их несанкционированной модификации, уничто-

---

[1] Конституция Российской Федерации. 1993. Ст. 41, п. 1.

[2] Основы законодательства Российской Федерации об охране здоровья граждан от 22 июля 1993 г.

[3] Доктрина информационной безопасности Российской Федерации. Утв. поручением Президента Российской Федерации от 9 сентября 2000 г.

жении или задержке. Эта угроза проявляется в форме соответствующих действий физических или юридических лиц.

В *основу правового регулирования отношений* в области противодействия данной угрозе положены следующие принципы:

– выделение социально опасных действий, направленных на нарушение безопасности сообщений (документов), передаваемых по каналам связи, данных, накапливаемых и обрабатываемых в информационных системах, в автоматизированных системах управления, и запрет этих действий под угрозой применения уголовной или административной ответственности;

– формирование механизмов установления, поддержания и снятия режимов общедоступной информации и информации органического доступа, в том числе режима тайны (коммерческой, государственной и иных охраняемых законом тайн);

– закрепление требований к информационным системам, техническим средствам передачи, обработка и хранение информации, контроль выполнения этих требований, а также установление в определенных случаях гражданской, административной и уголовной ответственности за нарушение этих требований;

– правовая охрана установленных режимов доступа к информации.

Правовое обеспечение безопасности информационной инфраструктуры образуется совокупностью правовых норм и институтов, регулирующих отношения, объектами которых являются средства связи, автоматизации обработки информации, информационно-телекоммуникационные системы и средства массовой информации.

Основные угрозы безопасности информационной инфраструктуры представляют собой нарушения работоспособности и функционирования основных составляющих информационной инфраструктуры — информационных и телекоммуникационных систем, сетей связи, системы массовой информации и т. п.

Основной целью правового обеспечения безопасности информационной инфраструктуры является предупреждение, пресечение и минимизация последствий проявления этих угроз.

В *основу правового регулирования отношений*, связанных с обеспечением безопасности *сети связи*, *средств автоматизации обработки информации* и *информационно-телекоммуникационных систем* как средства взаимодействия между отдельными субъектами, положены принципы:

– установление правового режима радиочастотного спектра и государственный контроль его поддержания;

– закрепление требований к организации защиты объектов и сооружений связи и установление административной ответственности за их выполнение;

– лицензирование деятельности по предоставлению услуг связи и государственный контроль за соблюдением лицензионных условий;

– подтверждение соответствия средств связи и услуг установленным требованиям;

– запрет на распространение вредоносных программ и применение уголовной ответственности за его нарушения.

В *основу правового регулирования отношений* в области обеспечения безопасности функционирования ***средств массовой информации*** и ***информационно-телекоммуникационных систем*** как средства распространения массовой информации положены принципы:

– ограничение участия иностранных юридических лиц, лиц с двойным гражданством и лиц без гражданства в учреждении российских средств массовой информации;

– запрет на распространение продукции зарубежных средств массовой информации вместо продукции отечественных средств массовой информации в качестве одного из условий получения лицензии на вещание, распространение продукции средств массовой информации[1], возможность аннулирования лицензии на вещание в случае неоднократного нарушения лицензионных условий;

– запрет на осуществление гражданами, должностными лицами, предприятиями, учреждениями, организациями, государственными органами действий, направленных на воспрепятствование распространению продукции СМИ, и привлечение виновных лиц к установленной законом административной ответственности[2].

Правовое обеспечение безопасности правового статуса субъектов информационной сферы образуется совокупностью правовых норм и институтов, регулирующих отношения, объектами которых являются:

– права человека и гражданина на участие в информационных отношениях (на свободу поиска, получения, передачи, производства и распространения информации, на свободу мысли и слова, массовой информации; на неприкосновенность частной жизни, личную и семейную тайну, на защиту своей чести и доброго имени, на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений и др.);

– обязанности граждан, возникающие в связи с участием в информационных отношениях (непротиводействие реализации конституционных прав и свобод в области информации; соблюдение запретов пропаганды и агитации, возбуждающих расовую, национальную, религиозную ненависть и вражду; забота о сохранении культурного наследия).

---

[1] Закон Российской Федерации «О средствах массовой информации». Ст. 31.

[2] Кодекс Российской Федерации об административных правонарушениях. Ст. 13, 16.

Основными угрозами безопасности правового статуса субъектов информационной сферы являются нерациональное ограничение доступа к общественно необходимой информации, открытым информационным ресурсам федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, органов местного самоуправления, к открытым архивным материалам, другой открытой социально значимой информации, манипулирование информацией, противодействие реализации гражданами их права на личную и семейную тайны, тайну переписки, телефонных переговоров и иных сообщений, а также нарушение других законных ограничений на сбор и распространение информации.

Основной целью правового обеспечения безопасности правового статуса субъектов информационной сферы является предупреждение, пресечение и минимизация последствий проявления этих угроз.

В *основу правового регулирования отношений*, связанных с обеспечением безопасности правового статуса субъектов информационной сферы, положены следующие принципы:

– закрепление государственных гарантий доступа к общедоступной информации, в том числе к информации о деятельности государственных органов, органов местного самоуправления;

– установление требований к созданию и функционированию государственных информационных систем и информационных систем органов местного самоуправления;

– законодательное закрепление порядка и условий автоматизированной обработки персональных данных;

– закрепление порядка использования электронной цифровой подписи в электронном документообороте для обмена юридически значимыми электронными документами.

6.2. Содержание и структура законодательства

Правовые нормы и институты, образующие правовое обеспечение информационной безопасности, закрепляются в нормативных правовых актах, являющихся источниками права в этой области и составляющих соответствующее законодательство.

В ***Конституции Российской Федерации*** закреплены следующие права и свободы: право каждого свободно искать, получать, передавать, производить и распространять информацию любым законным способом; право на неприкосновенность частной жизни, личную и семейную тайну; право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений; возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы; запрет на сбор,

хранение и распространение информации о частной жизни лица без его согласия и другие нормы.

Федеральные законы закрепляют значительное количество норм, регулирующих отношения в области обеспечения информационной безопасности. К числу данных законов относятся Федеральный конституционный закон «О Правительстве Российской Федерации», Федеральный конституционный закон «Об Уполномоченном по правам человека в Российской Федерации», Гражданский кодекс Российской Федерации, Уголовный кодекс Российской Федерации, Налоговый кодекс Российской Федерации, Трудовой кодекс Российской Федерации, Таможенный кодекс Российской Федерации и др.

Так, Гражданский кодекс Российской Федерации закрепляет нормы, регулирующие отношения в области защиты конфиденциальной информации и некоторых иных видов тайн (коммерческой тайны, личной и семейной тайны), признания электронной цифровой подписи средством удостоверения сделки.

Кодекс Российской Федерации об административных правонарушениях устанавливает ответственность за отказ в предоставлении гражданину информации, за нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных), за нарушение правил защиты информации, за незаконную деятельность в области защиты информации и другие некоторые правонарушения.

Уголовный кодекс Российской Федерации устанавливает ответственность за нарушение неприкосновенности частной жизни, тайны переписки и телефонных переговоров, отказ в предоставлении гражданину информации, незаконный экспорт научно-технической информации, разглашение государственной тайны, преступления в сфере компьютерной информации и другие преступления в данной сфере.

Важную роль в правовом регулировании отношений в области обеспечения информационной безопасности играют такие основополагающие нормативные правовые акты, как законы Российской Федерации «О безопасности», «О средствах массовой информации», «О государственной тайне», Патентный закон Российской Федерации, федеральные законы «Об информации, информационных технологиях и о защите информации», «Об электронной цифровой подписи» и др.

Среди ***нормативных правовых актов Президента Российской Федерации*** можно выделить указы Президента Российской Федерации «О снятии ограничительных грифов с законодательных и иных актов, служивших основанием для массовых репрессий и посягательств на права человека», «О дополнительных правах граждан на информацию», «О порядке опубликования и вступления в силу актов Президента Российской Федерации, Правительства

Российской Федерации и нормативных правовых актов федеральных органов исполнительной власти» и др. Кроме того, важной составляющей рассматриваемого законодательства являются указы Президента Российской Федерации, устанавливающие компетенцию федеральных органов исполнительной власти в рассматриваемой области.

Подзаконные акты Правительства Российской Федерации, других федеральных органов исполнительной власти, принятые по отнесенным к их компетенции вопросам и относящиеся к предмету правового обеспечения информационной безопасности, в частности, включают постановления Правительства Российской Федерации «Об упорядочении использования радиоэлектронных средств (высокочастотных устройств) на территории Российской Федерации», «О порядке изготовления, приобретения, ввоза в Российскую Федерацию и использования на территории Российской Федерации радиоэлектронных средств (высокочастотных устройств)», «О лицензировании деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны», «Об утверждении Положения о лицензировании деятельности физических и юридических лиц, не уполномоченных на осуществление оперативно-розыскной деятельности, связанной с разработкой, производством, реализацией, приобретением в целях продажи, ввоза в Российскую Федерацию и вывоза за ее пределы специальных технических средств, предназначенных (разработанных, приспособленных, запрограммированных) для негласного получения информации, и перечня видов специальных технических средств, предназначенных (разработанных, приспособленных, запрограммированных) для негласного получения информации в процессе осуществления оперативно-розыскной деятельности» и др.

Существует значительное количество правовых актов, принятых Гостехкомиссией России (в настоящее время функции уполномоченного федерального органа исполнительной власти в этой области исполняет ФСТЭК России) по вопросам защиты информации. Так, вопросы защиты информации затрагиваются в руководящих документах Гостехкомиссии России («Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации» 1992 г., «Защита от НСД. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровням контроля отсутствия недекларированных возможностей» 1998 г. и др.).

Кроме того, к источникам права в этой области могут относиться решения Конституционного Суда Российской Федерации,

разъяснения Верховного Суда Российской Федерации и Высшего Арбитражного Суда Российской Федерации.

Важной составляющей законодательства в области обеспечения информационной безопасности являются также международные договоры Российской Федерации.

Структура законодательства в области правового обеспечения информационной безопасности и структура нормативного правового обеспечения информационной безопасности в определенной степени различаются. Это обусловлено тем, что система права и система законодательства, образуя совместно объективное право, имеют разные назначение и механизмы развития. В системе права отражается содержание права как регулятивной системы, состоящей из норм права, правовых институтов и отраслей права. Она выступает объективным основанием системы законодательства.

В свою очередь, система законодательства призвана закрепить правовые нормы в системе нормативных правовых актов, взаимосвязанных по предмету правового регулирования и их юридической силе.

В отличие от системы права, складывающейся в соответствии с исторически обусловленной структурой общественных отношений, система законодательства является продуктом рациональной деятельности людей, осуществляемой во времени и пространстве.

Система законодательства, как и система права, подразделяется на отрасли — наиболее крупные объединения нормативных актов и их частей по определенным сферам правового регулирования.

Элементами системы законодательства являются нормативные правовые акты, а также их структурные составляющие (разделы, главы, статьи пункты и т.д.), которые могут объединяться в различные композиции, выделенные по определенному основанию из всей совокупности признаков и характеристик объекта.

Структуру законодательства в области обеспечения информационной безопасности удобно представлять в качестве системы законодательных отраслей права, включающих, в частности:

– законодательство об информации, информационных технологиях и о защите информации;
– законодательство о персональных данных;
– законодательство об интеллектуальной собственности;
– законодательство о тайнах;
– законодательство о средствах массовой информации и о рекламе;
– законодательство о связи;
– законодательство о техническом регулировании;
– законодательство об электронной цифровой подписи.

Контрольные вопросы

1. Что такое «правовое обеспечение информационной безопасности» и в чем заключается его предмет?
2. Раскройте содержание правового обеспечения безопасности сведений.
3. Опишите содержание правового обеспечения безопасности сообщений
4. Раскройте содержание правового обеспечения безопасности информационной инфраструктуры.
5. Расскажите о правовом обеспечении безопасности правового статуса субъекта информационной сферы.
6. Раскройте содержание и структуру законодательства в области обеспечения информационной безопасности.

Глава 7

ЗАКОНОДАТЕЛЬСТВО ОБ ИНФОРМАЦИИ, ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЯХ И О ЗАЩИТЕ ИНФОРМАЦИИ

7.1. Общие положения

Законодательство Российской Федерации об информации, информационных технологиях и о защите информации состоит из Федерального закона «Об информации, информационных технологиях и о защите информации» и других федеральных законов, регулирующих отношения в области использования информации.

Предметом правового регулирования в области информации, информационных технологий и защиты информации являются отношения, возникающие при осуществлении права на поиск, получение, передачу, производство и распространение информации; при применении информационных технологий; при обеспечении защиты информации.

Цель правового регулирования заключается в защите прав и свобод человека и гражданина в области доступа к информации, информационным технологиям, а также защиты информации от неправомерных действий.

С этой целью законодательно закрепляются правовые режимы информации и информационных технологий, правовой статус обладателя информации, а также институт защиты информации.

Основными принципами правового регулирования отношений, возникающих в рассматриваемой сфере, являются:

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

– установление ограничений доступа к информации только федеральными законами;

– открытость информации о деятельности государственных органов, 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;

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

– достоверность информации и своевременность ее предоставления;

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

– 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.

7.2. Правовой режим информации

Объектом рассматриваемого правового режима является *информация*, под которой в законодательстве понимаются сведения (сообщения, данные) независимо от формы их представления.

Информация, зафиксированная на материальном носителе путем документирования, с реквизитами, позволяющими определить такую информацию или в установленных законодательством Российской Федерации случаях ее материальный носитель, называется *документированной информацией.*

Одной из важных форм документированной информации является *электронное сообщение* — информация, переданная или полученная пользователем информационно-телекоммуникационной сети.

Правовой режим информации включает:

– право использования информации в качестве объекта правовых отношений;

– право обладания информацией;

– право доступа к информации;

– право собственности и иные вещные права на магнитные носители, содержащие документированную информацию;

– документирование информации;

– право распространения и предоставления информации.

Право использования информации в качестве объекта правовых отношений заключается в возможности установления публичных, гражданских и иных правовых отношений, объектом которых является информация.

Законодательством установлено, что в целях заключения гражданско-правовых договоров или оформления иных правоотношений 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.*

Электронное сообщение, подписанное электронной цифровой подписью или иным аналогом собственноручной подписи, при-

знается *электронным документом*, равнозначным документу, подписанному собственноручной подписью, в случаях, если федеральными законами или иными нормативными правовыми актами не устанавливается или не подразумевается требование о составлении такого документа на бумажном носителе.

Право обладания информацией заключается в возможности распоряжения ею (разрешение или ограничение доступа; использование, включая распространение; передача другим лицам; правовая защита и иные действия) по усмотрению обладателя.

Право доступа к информации заключается в возможности ее свободного получения и использования любым лицом и передачи одним лицом другому лицу, в случае 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 и информацию ограниченного доступа.

К *общедоступной информации* относятся общеизвестные сведения и иная информация, 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.

Условия отнесения к *информации ограниченного доступа* сведений, составляющих коммерческую, служебную и иную тайну, устанавливаются федеральными законами.

Граждане (физические лица) 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 законодательством.

Гражданин (физическое лицо) 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 уставной деятельности.

Законодательством установлен *запрет на ограничение доступа*:

– 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.

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 федеральными законами.

Законодательством установлено, что ***право собственности и иные вещные права на материальные носители, содержащие документированную информацию***, устанавливаются гражданским законодательством. Это означает, что такие носители являются объектами гражданских прав наряду с другими вещами.

Документирование информации как составляющая правового режима информации заключается в том, что недокументированная информация преобразуется в документированную в соответствии с требованиями, устанавливаемыми законодательством Российской Федерации или соглашением сторон.

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.

Право распространения и предоставления информации заключается в возможности свободного осуществления действий, направленных на получение информации неопределенным кругом лиц или на передачу информации неопределенному кругу лиц (распространение), и действий, направленных на получение информации определенным кругом лиц или на передачу информации определенному кругу лиц (предоставление), при соблюдении требований, установленных законодательством Российской Федерации.

Информацию в *зависимости от порядка ее предоставления или распространения* подразделяют на свободно распространяемую; предоставляемую по соглашению лиц, участвующих в соответствующих отношениях; подлежащую в соответствии с федеральными законами предоставлению или распространению; распространяемую в Российской Федерации ограниченно или запрещаемую к распространению.

К *требованиям, предъявляемым к распространению и предоставлению информации*, относят:

– включение в информацию, распространяемую без использования средств массовой информации, достоверных сведений о ее обладателе или об ином лице, распространяющем информацию, в форме и объеме, которые достаточны для идентификации такого лица;

– обеспечение получателю информации лицом, распространяющим информацию, возможности отказа от нее при использовании для распространения средств, позволяющих определять получателей информации, в том числе почтовых отправлений и электронных сообщений;

– установление соглашения, определяющего порядок предоставления информации, между лицами, участвующими в обмене информацией;

– запрет распространения 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.

Случаи и условия обязательного распространения информации или предоставления информации, в том числе обязательных экземпляров документов, устанавливаются федеральными законами.

Законодательством Российской Федерации могут быть установлены виды информации в зависимости от ее содержания или обладателя.

7.3. Правовой статус обладателя информации

Обладателем информации считается лицо (физическое или юридическое лицо, Российская Федерация, субъект Российской Федерации, муниципальное образование), самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам.

От имени Российской Федерации, субъекта Российской Федерации, муниципального образования правомочия обладателя информации осуществляются соответственно государственными орга-

нами и органами местного самоуправления в пределах их полномочий, установленных соответствующими нормативными правовыми актами.

Обладатель информации, если иное не предусмотрено 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.

При осуществлении своих прав обладатель информации *обязан*:

– соблюдать права и законные интересы иных лиц;

– принимать меры по защите информации;

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

Обладатель информации, ставшей по его решению общедоступной, вправе требовать от лиц, распространяющих такую информацию, указывать себя в качестве источника такой информации.

Обладатель информации обязан обеспечить бесплатное предоставление: информации о деятельности государственных органов и органов местного самоуправления, если она размещена этими субъектами в информационно-телекоммуникационных сетях; информации, затрагивающей права и установленные законодательством Российской Федерации обязанности заинтересованного лица; иной установленной законом информации.

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.

7.4. Правовой режим информационных технологий

Объектом правового режима являются информационные технологии, представляющие собой процессы и(или) методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

Информационные технологии реализуются в форме информационных систем и информационно-телекоммуникационных сетей.

Информационная система представляет собой совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств, а информационно-телекоммуникационная сеть — технологическую систему, предназначенную для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники.

Различают следующие *виды информационных систем*:

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

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

– иные информационные системы.

Если иное не установлено федеральными законами, то 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.

Под *оператором информационной системы* понимается гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных.

Права обладателя информации, содержащейся в базах данных информационной системы, подлежат охране независимо от авторских и иных прав на такие базы данных.

Установленные законодательством 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 законодательством.

Правовой режим информационных технологий включает:

– перечень областей государственного регулирования в сфере применения информационных технологий;

– требования к государственным информационным системам;

– порядок регулирования использования информационно-коммуникационных сетей.

Перечень областей государственного регулирования в сфере применения информационных технологий включает:

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

– 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.

Требования к государственным информационным системам включают требования к целям и условиям их создания и эксплуатации.

Установлено, что 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 с учетом* требований, предусмотренных Федеральным законом от 21 июля 2005 г. № 94-ФЗ «О размещении заказов на поставки товаров, выполнение работ, оказание услуг для государственных и муниципальных нужд».

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 пре-

доставления информации — Правительством Российской Федерации или соответствующими государственными органами, если иное не предусмотрено федеральными законами.

Если иное не установлено решением о создании государственной информационной системы, функции ее оператора осуществляются заказчиком, заключившим государственный контракт на создание такой информационной системы. При этом ввод государственной информационной системы в эксплуатацию осуществляется в порядке, установленном указанным заказчиком.

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.

Технические средства, предназначенные для обработки информации, содержащейся в государственных информационных системах, в том числе программно-технические средства и средства защиты информации, должны соответствовать требованиям законодательства Российской Федерации о техническом регулировании.

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

Порядок регулирования использования информационно-телекоммуникационных сетей на территории Российской Федерации устанавливается законодательством Российской Федерации в области связи, информации, информационных технологий, защиты информации 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 Федеральным законом.

Использование на территории Российской Федерации информационно-телекоммуникационных сетей в хозяйственной или иной деятельности не может служить основанием для установления дополнительных требований или ограничений, касающихся регулирования указанной деятельности, осуществляемой без использования таких сетей, а также для несоблюдения требований, установленных федеральными законами.

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 Российской Федерации, вправе провести проверку, позволяющую установить отправителя электронного сообщения, а в установленных федеральными законами или соглашением сторон случаях обязан провести такую проверку.

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

Особенности подключения государственных информационных систем к информационно-телекоммуникационным сетям могут быть установлены нормативным правовым актом Президента Российской Федерации или нормативным правовым актом Правительства Российской Федерации.

7.5. Защита информации

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.

Государственное регулирование отношений в сфере защиты информации осуществляется путем установления требований о защите информации, а также ответственности за нарушение законодательства Российской Федерации об информации, информационных технологиях и о защите информации.

Требования о защите общедоступной информации могут устанавливаться только для достижения указанных выше целей.

Обладатель информации и *оператор информационной системы* в случаях, установленных законодательством Российской Федерации, *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 к 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 используемые в целях защиты информации методы и способы ее защиты должны соответствовать указанным требованиям.

Федеральными законами могут быть установлены ограничения на использование определенных средств защиты информации и на осуществление отдельных видов деятельности в области защиты информации.

Контрольные вопросы

1. В чем заключаются предмет и цель правового регулирования в области информации, информационных технологий и защиты информации?
2. Раскройте содержание правового режима информации.
3. Опишите содержание правового статуса обладателя информации.
4. Расскажите о правовом режиме информационных технологий.
5. Раскройте содержание деятельности по защите информации.

Глава 8

ЗАКОНОДАТЕЛЬСТВО О ПЕРСОНАЛЬНЫХ ДАННЫХ

8.1. Общие положения

Законодательство в области персональных данных состоит из Федерального закона «О персональных данных» и других федеральных законов, определяющих случаи и особенности обработки персональных данных.

Предметом правового регулирования в области персональных данных являются отношения, связанные с обработкой этих данных с применением средств автоматизации или без их применения.

Исключение составляют отношения, возникающие:

– в связи с обработкой персональных данных физическими лицами для личных и семейных нужд;

– при формировании и использовании Архивного фонда Российской Федерации;

– при формировании и использовании единого государственного реестра индивидуальных предпринимателей;

– в случае, если эти данные составляют государственную тайну.

Под ***персональными данными*** понимается любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

К *особым категориям персональных данных* относится информация о субъекте, касающаяся расы, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни, а также физиологических особенностей, на основании которых можно установить его личность (***биометрические персональные данные***).

Цель правового регулирования заключается в обеспечении защиты прав и свобод человека и гражданина при обработке персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайны. Основные угрозы безопасности этих прав и свобод заключаются в неправомерном использовании собираемых персональных данных государственными органами, органами местного самоуправления, юридическими и физическими лицами.

В целях противодействия указанной угрозе *законодательно закрепляются*:

– принципы и условия обработки персональных данных и их конфиденциальность;

– права субъектов персональных данных;

– обязанности оператора при обработке персональных данных;

– механизм контроля и надзора за соблюдением законодательства.

Под *оператором* понимается государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки этих данных.

8.2. Принципы и условия обработки персональных данных, их конфиденциальность

Обработка персональных данных должна осуществляться на основе следующих ***принципов***:

– законность целей и способов обработки персональных данных и добросовестность;

– соответствие целей обработки заранее объявленным и заявленным при сборе персональных данных, а также полномочиям оператора;

– соответствие объема и характера обрабатываемых персональных данных, способов их обработки заявленным целям;

– достоверность персональных данных, их достаточность для целей обработки и недопустимость их избыточности;

– недопустимость объединения созданных для несовместимых между собой целей баз данных информационных систем персональных данных;

– уничтожение персональных данных по достижении целей обработки или в случае утраты необходимости в достижении этих целей.

Основным условием обработки персональных данных является согласие субъекта этих данных, которое он дает своей волей и в своем интересе.

При составлении *общедоступных источников персональных данных* (в том числе справочников, адресных книг), специальных категорий персональных данных, биометрических персональных данных согласие должно быть дано в письменной форме и включать:

– фамилию, имя, отчество, адрес субъекта персональных данных, номер основного документа, удостоверяющего личность, сведения о дате выдачи документа и выдавшем его органе;

– наименование (фамилию, имя, отчество) и адрес оператора, получающего согласие субъекта персональных данных;

– цель обработки персональных данных;

– перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;

– перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых оператором способов обработки персональных данных;

– срок, в течение которого действует согласие, а также порядок его отзыва.

Предварительное согласие субъекта персональных данных на их использование является обязательным условием использования этих данных в целях продвижения товаров, работ, услуг на рынке путем осуществления прямых контактов с потенциальным потребителем с помощью средств связи.

Обязанность доказывать наличие согласия субъекта персональных данных на обработку или отнесение персональных данных к общедоступным лежит на операторе.

Согласие субъекта персональных данных не требуется в таких случаях:

– как обязательное предоставление таких данных в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства;

– обработка биометрических персональных данных в связи с осуществлением правосудия, а также в случаях, предусмотренных законодательством о безопасности, оперативно-розыскной деятельности, государственной службе, уголовно-исполнительным законодательством, законодательством о порядке выезда из Российской Федерации и въезда в нее;

– обработка персональных данных на основании федерального закона, устанавливающего ее цель, условия получения персональных данных и круг субъектов, персональные данные которых подлежат обработке, а также определяющего полномочия оператора;

– обработка персональных данных в целях исполнения договора, одной из сторон которого является субъект персональных данных;

– обработка персональных данных для статистических или иных научных целей при условии обязательного обезличивания персональных данных;

– обработка данных для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получено его согласие;

– обработка персональных данных для доставки почтовых отправлений организациями почтовой связи, осуществления операторами электросвязи расчетов с пользователями услуг связи;

– обработка персональных данных в целях профессиональной деятельности журналиста либо в целях научной, литературной или

иной творческой деятельности при условии, что не нарушаются права и свободы субъекта персональных данных;

– обработка персональных данных, подлежащих опубликованию в соответствии с федеральными законами.

Государственные и муниципальные органы создают в пределах своих полномочий *государственные* и *муниципальные информационные системы персональных данных*. Операторы и третьи лица, получающие доступ к персональным данным, должны обеспечивать их конфиденциальность, за исключением случаев обезличивания данных и обработки общедоступных данных.

8.3. Права субъектов персональных данных

Субъект персональных данных обладает правами:

– на доступ к своим персональным данным;

– возражение против принятия решений исключительно на основании автоматизированной обработки персоналом данных, порождающих юридические последствия в отношении субъекта или иным образом затрагивающих его права и законные интересы;

– обжалование действий или бездействий;

– отзыв согласия на обработку персональных данных.

Право на доступ к своим персональным данным включает:

– получение сведений об операторе, месте его нахождения, наличии у оператора соответствующих персональных данных, а также ознакомление с ними;

– получение сведений, касающихся обработки персональных данных;

– уточнение своих персональных данных, их блокирование или уничтожение в случае, если эти данные являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки.

Доступ должен быть предоставлен как лично субъекту персональных данных, так и его законному представителю по обращению или запросу этих лиц. Обращение и запрос могут быть отправлены в электронной форме и подписаны электронной цифровой подписью.

Правомочие получения информации, касающейся обработки персональных данных, реализуется субъектом этих данных посредством обращения или запроса. В *рамках ответа на обращение* или *запрос* субъект имеет право на ответ, содержащий следующую информацию:

– подтверждение факта обработки персональных данных, применяемых оператором;

– способы обработки персональных данных, применяемые оператором;

– сведения о лицах, которые имеют доступ к персональным данным или которым может быть предоставлен такой доступ;

– перечень обрабатываемых персональных данных и источник их получения;

– срок обработки персональных данных, в том числе сроки их хранения;

– сведения о том, какие юридические последствия для субъекта персональных данных может повлечь за собой обработка его персональных данных.

Пользование этим правомочием ограничивается, если:

– обработка персональных данных, полученных в результате оперативно-розыскной, контрразведывательной и разведывательной деятельности, осуществляется в целях обороны страны, безопасности государства и охраны правопорядка;

– обработка проводится органами, осуществившими задержание субъекта персональных данных по подозрению в совершении преступления либо предъявившими субъекту персональных данных меру пресечения до предъявления обвинения, за исключением предусмотренных уголовно-процессуальным законодательством случаев, когда допускается ознакомление подозреваемого или обвиняемого с такими персональными данными;

– представление персональных данных нарушает конституционные права и свободы других лиц.

Право на возражение против принятия решений исключительно на основании автоматизированной обработки персональных данных, порождающих юридические последствия в отношении субъекта или иным образом затрагивающих его права и законные интересы, заключается в следующем:

– получение у оператора разъяснений о порядке принятия таких решений и о их возможных юридических последствиях;

– подача заявления о возражении против такого решения;

– получение у оператора разъяснений о порядке защиты субъектом своих прав и законных интересов;

– получение уведомления от оператора о результатах рассмотрения возражения.

Право на обжалование действий или бездействий включает:

– обжалование действия или бездействия оператора, нарушающие права и свободы субъекта персональных данных, в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке;

– возмещение убытков и компенсации морального вреда в судебном порядке.

Право на отзыв согласия на обработку персональных данных заключается в возможности запретить соответствующие действия оператора в отношении своих персональных данных. В этом случае оператор обязан прекратить обработку персональных данных и уничтожить их в срок, не превышающий трех рабочих дней с даты поступления указанного отзыва, если иное не предусмотрено со-

глашением между оператором и субъектом персональных данных. Об уничтожении персональных данных оператор обязан уведомить субъекта персональных данных.

8.4. Обязанности оператора при обработке персональных данных

При обработке персональных данных на оператора возлагаются следующие обязанности: по соблюдению установленного порядка сбора персональных данных; по обеспечению безопасности; по реагированию на обращения и запросы; по устранению нарушений законодательства; по уведомлению об обработке персональных данных.

Обязанности по соблюдению установленного порядка сбора персональных данных заключаются в следующем:

– предоставление по просьбе субъекта персональных данных информации, касающейся обработки его персональных данных;

– представление в случае получения персональных данных не от субъекта этих данных (за исключением случаев их представления на основании федерального закона или когда они являются общедоступными) субъекту персональных данных до начала их обработки следующей информации, наименование (фамилия, имя, отчество) и адрес оператора или его представителя; цель обработки персональных данных и ее правовое основание; предполагаемые пользователи персональных данных; установленные законом права субъекта персональных данных.

Обязанности по обеспечению безопасности персональных данных включают:

– принятие необходимых организационных и технических мер, в том числе связанных с использованием шифровальных (криптографических) средств, для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также от иных неправомерных действий;

– использование и хранение биометрических персональных данных вне информационных систем персональных данных только на материальных носителях информации и с применением таких технологий ее хранения, которые обеспечивают защиту этих данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения.

Обязанности по реагированию на обращения и запросы заключаются в следующем:

– сообщение субъекту персональных данных или его законному представителю информации о наличии персональных данных, относящихся к соответствующему субъекту персональных данных, а также предоставление возможности ознакомления с этими дан-

ными при обращении или запросе субъекта персональных данных или его законного представителя;

– предоставление в письменной форме мотивированного ответа, содержащего ссылку на положения федеральных законов, являющиеся основанием для отказа в предоставлении информации о наличии персональных данных о соответствующем субъекте персональных данных;

– безвозмездное предоставление субъекту персональных данных или его законному представителю возможности ознакомления с персональными данными, относящимися к субъекту персональных данных;

– внесение в персональные данные необходимых изменений, уничтожение или блокирование соответствующих персональных данных по представлению субъектом персональных данных или его законным представителем сведений, подтверждающих, что персональные данные, обработку которых осуществляет оператор, являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки;

– уведомление субъекта персональных данных или его законного представителя и третьих лиц, которым персональные данные этого субъекта были переданы, о внесенных изменениях и предпринятых мерах;

– сообщение в уполномоченный орган по защите прав субъектов персональных данных по его запросу информации, необходимой для осуществления деятельности указанного органа.

Обязанности по устранению нарушений законодательства включают:

– блокирование персональных данных, относящихся к соответствующему субъекту при обращении или по запросу субъекта персональных данных или его законного представителя в случае выявления недостоверных персональных данных или неправомерных действий с ними оператора;

– уточнение персональных данных и снятие с них блокирования на основании документов, представленных субъектом персональных данных или его законным представителем либо уполномоченным органом по защите прав субъектов персональных данных;

– устранение выявленных нарушений в срок, не превышающий трех дней с даты выявления неправомерных действий с персональными данными, либо уничтожение этих данных;

– уведомление субъекта персональных данных или его законного представителя об устранении допущенных нарушений или об уничтожении соответствующих персональных данных;

– прекращение обработки персональных данных и уничтожение их в случае достижения цели обработки, а также в случае отзыва субъектом персональных данных согласия на их обработку.

Обязанности по уведомлению об обработке персональных данных заключаются в уведомлении уполномоченного органа по защите прав субъектов персональных данных о своем намерении осуществлять обработку персональных данных до начала их обработки.

Обработка персональных данных может осуществляться *без уведомления уполномоченного органа по защите персональных данных*, если эти данные:

– относятся к субъектам персональных данных, связанным с оператором трудовыми отношениями;

– получены оператором в связи с заключением договора, стороной которого является субъект персональных данных, если персональные данные не распространяются, а также не предоставляются третьим лицам и используются оператором исключительно для исполнения указанного договора и заключения договоров с субъектом персональных данных;

– относятся к членам общественного объединения или религиозной организации и обрабатываются соответствующими общественными объединениями или религиозными организациями, действующими в соответствии с законодательством, для достижения целей, предусмотренных их учредительными документами;

– являются общедоступными;

– включают только фамилии, имена, отчества субъектов персональных данных;

– необходимы для однократного пропуска субъекта персональных данных на территорию, на которой находится оператор;

– включены в информационные системы персональных данных, имеющие в соответствии с федеральными законами статус федеральных автоматизированных информационных систем, а также в государственные информационные системы персональных данных, созданные для защиты безопасности государства и общественного порядка;

– обрабатываются без использования средств автоматизации в соответствии с федеральными законами или иными нормативными актами, устанавливающими требования к обеспечению безопасности персональных данных при их обработке.

8.5. Контроль и надзор

Контроль и надзор за соответствием обработки персональных данных требованиям законодательства осуществляются уполномоченным органом по защите прав субъектов персональных данных. Таковым является федеральный орган исполнительной власти, выполняющий функции по контролю и надзору в сфере информационных технологий и связи.

Субъекты персональных данных, полагающие что их права и законные интересы нарушены оператором в связи с нарушением

требований законодательства по содержанию персональных данных, способам и целям их обработки, имеют право направить обращение в уполномоченный орган по защите персональных данных. Уполномоченный орган по результатам рассмотрения обращений принимает соответствующее решение, которое может быть обжаловано в судебном порядке.

В целях выполнения возложенных функций ***уполномоченный орган по защите прав субъектов персональных данных имеет право***:

– запрашивать у физических и юридических лиц информацию, необходимую для реализации своих полномочий, и безвозмездно получать ее;

– осуществлять проверку сведений, содержащихся в уведомлении об обработке персональных данных, или привлекать для осуществления такой проверки иные государственные органы в пределах их полномочий;

– требовать от оператора уточнения, блокирования или уничтожения недостоверных или полученных незаконным путем персональных данных;

– принимать в установленном законодательством порядке меры по приостановлению или прекращению обработки персональных данных, если такая обработка осуществляется с нарушением требований законодательства;

– обращаться в суд с исковыми заявлениями в защиту прав субъектов персональных данных и представлять интересы субъектов персональных данных в суде;

– направлять заявления в орган, осуществляющий лицензирование деятельности оператора, для рассмотрения вопроса о принятии мер по приостановлению действия или аннулированию соответствующей лицензии;

– направлять в органы прокуратуры, другие правоохранительные органы материалы для решения вопроса о возбуждении уголовных дел по признакам преступлений, связанных с нарушением прав субъектов персональных данных;

– привлекать к административной ответственности лиц, виновных в нарушении законодательства в области персональных данных.

При выполнении своих функций ***уполномоченный орган по защите прав субъектов персональных данных обязан***:

– организовывать в соответствии с требованиями законодательства защиту прав субъектов персональных данных;

– рассматривать жалобы и обращения граждан и юридических лиц по вопросам, связанным с обработкой персональных данных, а также принимать в пределах своих полномочий решения по результатам их рассмотрения;

– вести реестр операторов;

– осуществлять меры, направленные на совершенствование защиты прав субъектов персональных данных;

– принимать в установленном порядке по представлению федерального органа исполнительной власти, уполномоченного в области обеспечения безопасности, или федерального органа исполнительной власти, уполномоченного в области противодействия техническим разведкам и технической защиты информации, меры по приостановлению или прекращению обработки персональных данных;

– информировать государственные органы, а также субъектов персональных данных по результатам их обращений или запросов о положении дел в области защиты прав субъектов персональных данных.

Отчет о своей деятельности уполномоченный орган по защите прав субъектов персональных данных ежегодно направляет Президенту Российской Федерации, в Правительство Российской Федерации и Федеральное Собрание Российской Федерации. Отчет подлежит опубликованию в средствах массовой информации.

При уполномоченном органе по защите прав субъектов персональных данных создается на общественных началах консультативный совет.

Контрольные вопросы

1. Что составляет предмет и в чем заключается цель правого регулирования в области персональных данных?
2. Раскройте принципы и условия обработки персональных данных, их конфиденциальность.
3. Изложите содержание прав субъектов персональных данных.
4. Раскройте содержание обязанностей оператора при обработке персональных данных.
5. Расскажите об организации контроля и надзора соблюдения законодательства в области персональных данных.

Глава 9

ЗАКОНОДАТЕЛЬСТВО В ОБЛАСТИ ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

9.1. Общие положения

Законодательство в области интеллектуальной собственности образуется совокупностью положений части четвертой Гражданского кодекса Российской Федерации, международных договоров Российской Федерации, других нормативных правовых актов, регулирующих отношения в области интеллектуальной собственности.

Под *интеллектуальной собственностью* понимаются результаты интеллектуальной деятельности и приравненные к ним средства индивидуализации юридических лиц, товаров, работ, услуг и предприятий, которым предоставляется правовая охрана.

Основными объектами интеллектуальной собственности являются: произведения науки, литературы и искусства; программы для электронных вычислительных машин (программы для ЭВМ); базы данных; исполнения; фонограммы; сообщение в эфир или по кабелю радио- или телепередач (вещание организаций эфирного или кабельного вещания); изобретения; полезные модели; промышленные образцы; селекционные достижения; топологии интегральных микросхем; секреты производства (ноу-хау); фирменные наименования; товарные знаки и знаки обслуживания; наименования мест происхождения товаров; коммерческие обозначения.

Предмет правового регулирования в рассматриваемой области составляют общественные отношения, возникающие в связи с правовой охраной интеллектуальных прав на объекты интеллектуальной собственности.

Интеллектуальные права включают исключительные права, являющиеся имущественным правом, личные, неимущественные права и иные права в случаях, предусмотренных законодательством.

Исключительное право — охраняемая правом возможность правообладателя по своему усмотрению любым не противоречащим закону способом использовать объект интеллектуальной собственности, результат интеллектуальной деятельности или средство индивидуализации, распоряжаться им, разрешать или запрещать другим лицам его использование.

Исключительное право на объект интеллектуальной деятельности первоначально возникает у автора — гражданина, творче-

ским трудом которого создан данный объект. Автору принадлежат право авторства и в установленных законодательством случаях — право на имя и иные личные неимущественные права.

Правообладатель может распорядиться принадлежащим ему исключительным правом на результат интеллектуальной деятельности, например, путем его отчуждения по договору другому лицу (*договор об отчуждении исключительного права*) или предоставления другому лицу права использования соответствующих результатов интеллектуальной деятельности и средств индивидуализации в установленных договором пределах (*лицензионный договор*).

Правовая охрана объектов интеллектуальной собственности осуществляется прежде всего на основе следующих относительно самостоятельных институтов гражданского права: авторского права; прав смежных с авторскими; патентного права; права на селекционное достижение; права на топологию интегральных микросхем; права на секрет производства (ноу-хау); права на средства индивидуализации юридических лиц, товаров, работ, услуг и предприятий; права на использование результатов интеллектуальной деятельности в составе единой технологии.

В пособии содержание права на селекционное достижение не рассматривается.

9.2. Авторское право и смежные права

Авторские права — это интеллектуальные права на произведения науки, литературы и искусства.

Объектами авторских прав являются: литературные произведения; драматические и музыкально-драматические произведения, сценарные произведения; хореографические произведения и пантомимы; музыкальные произведения с текстом или без текста; аудиовизуальные произведения; произведения живописи, скульптуры, графики, дизайна, графические рассказы, комиксы и другие произведения изобразительного искусства; произведения декоративно-прикладного и сценографического искусства; произведения архитектуры, градостроительства и садово-паркового искусства, в том числе в виде проектов, чертежей, изображений и макетов; фотографические произведения и произведения, полученные способами, аналогичными фотографии; географические, геологические и другие карты, планы, эскизы и пластические произведения, относящиеся к географии, топографии и другим наукам; программы для ЭВМ, которые охраняются как литературные произведения; производные произведения, т.е. произведения, представляющие собой переработку другого произведения; составные произведения, т.е. произведения, представляющие собой по подбору или расположению материалов результат творческого труда.

Авторские права распространяются как на обнародованные, так и на необнародованные произведения, выраженные в какой-либо объективной форме, в том числе в письменной, устной форме (в виде публичного произнесения, публичного исполнения и иной подобной форме), изображения, звуко- или видеозаписи, в объемно-пространственной форме.

Для возникновения, осуществления и защиты авторских прав не требуются регистрация произведения или соблюдение каких-либо иных формальностей.

В отношении программ для ЭВМ и баз данных возможна регистрация, осуществляемая по желанию правообладателя.

Авторские права не распространяются на идеи, концепции, принципы, методы, процессы, системы, способы, решения технических, организационных или иных задач, открытия, факты, языки программирования.

Не являются объектами авторских прав: официальные документы государственных органов и органов местного самоуправления муниципальных образований, в том числе законы, другие нормативные акты, судебные решения, иные материалы законодательного, административного и судебного характера, официальные документы международных организаций, их официальные переводы; государственные символы и знаки (флаги, гербы, ордена, денежные знаки и тому подобное), а также символы и знаки муниципальных образований; произведения народного творчества (фольклор), не имеющие конкретных авторов; сообщения о событиях и фактах, имеющие исключительно информационный характер (сообщения о новостях дня, программы телепередач, расписания движения транспортных средств и тому подобное).

Авторские права распространяются на часть произведения, на его название, на персонаж произведения, если по своему характеру они могут быть признаны самостоятельным результатом творческого труда автора.

Авторские права на все виды программ для ЭВМ (в том числе на операционные системы и программные комплексы), которые могут быть выражены на любом языке и в любой форме, включая исходный текст и объектный код, охраняются так же, как авторские права на произведения литературы. *Программой для ЭВМ* является представленная в объективной форме совокупность данных и команд, предназначенных для функционирования ЭВМ и других компьютерных устройств в целях получения определенного результата, включая подготовительные материалы, полученные в ходе разработки программы для ЭВМ и порождаемые ею аудиовизуальные отображения.

Основные субъекты авторских прав — авторы и другие правообладатели.

Авторские права включают следующие составляющие: исключительное право на произведение; право авторства; право автора на имя; право на неприкосновенность произведения; право на обнародование произведения.

Исключительное право на произведение — это возможность автора произведения или иного правообладателя использовать произведение в любой форме и любым не противоречащим закону способом.

Право авторства — возможность признаваться автором произведения.

Право автора на имя — возможность использовать или разрешать использование произведения под своим именем, под вымышленным именем (псевдонимом) или без указания имени, т.е. анонимно.

Право на неприкосновенность произведения — возможность автора запретить внесение в его произведение изменений, сокращений и дополнений, снабжение произведения при его использовании иллюстрациями, предисловием, послесловием, комментариями или какими бы то ни было пояснениями (право на неприкосновенность произведения).

Право на обнародование произведения — возможность автора обнародовать свое произведение, т.е. осуществить действие или дать согласие на осуществление действия, которое впервые делает произведение доступным для всеобщего сведения путем его опубликования, публичного показа, публичного исполнения, сообщения в эфир или по кабелю либо любым другим способом.

Автор обладает *правом на отказ* от ранее принятого решения об обнародовании произведения (право на отзыв) при условии возмещения лицу, которому отчуждено исключительное право на произведение или предоставлено право использования произведения, причиненных таким решением убытков. Если произведение уже обнародовано, автор также обязан публично оповестить о его отзыве. При этом автор вправе изъять из обращения ранее выпущенные экземпляры произведения, возместив причиненные этим убытки.

Допускается без согласия автора или иного правообладателя и без выплаты вознаграждения воспроизведение гражданином исключительно в личных целях правомерно обнародованного произведения, кроме: воспроизведения произведений архитектуры в форме зданий и аналогичных сооружений; воспроизведения баз данных или их существенных частей; воспроизведения программ для ЭВМ, кроме случаев, установленных законодательством; репродуцирования (полностью) и нотных текстов; видеозаписи аудиовизуального произведения при его публичном исполнении в месте, открытом для свободного посещения, или в месте, где присутствует значительное число лиц, не принадле-

жащих к обычному кругу семьи; воспроизведения аудиовизуального произведения с помощью профессионального оборудования, не предназначенного для использования в домашних условиях.

Допускается без согласия автора или иного правообладателя и без выплаты вознаграждения, но с обязательным указанием имени автора, произведение которого используется, и источника заимствования:

– цитирование в оригинале и в переводе в научных, полемических, критических или информационных целях правомерно обнародованных произведений в объеме, оправданном целью цитирования, включая воспроизведение отрывков из газетных и журнальных статей в форме обзоров печати;

– использование правомерно обнародованных произведений и отрывков из них в качестве иллюстраций в изданиях, радио- и телепередачах, звуко- и видеозаписях учебного характера в объеме, оправданном поставленной целью;

– воспроизведение в прессе, сообщение в эфир или по кабелю правомерно опубликованных в газетах или журналах статей по текущим экономическим, политическим, социальным и религиозным вопросам или переданных в эфир произведений такого же характера в случаях, когда такое воспроизведение или сообщение не было специально запрещено автором или иным правообладателем;

– воспроизведение в прессе, сообщение в эфир или по кабелю публично произнесенных политических речей, обращений, докладов и других аналогичных произведений в объеме, оправданном информационной целью;

– воспроизведение или сообщение для всеобщего сведения в обзорах текущих событий средствами фотографии, кинематографии, путем сообщения в эфир или по кабелю произведений, которые становятся увиденными или услышанными в ходе таких событий, в объеме, оправданном информационной целью;

– воспроизведение без извлечения прибыли рельефно-точечным шрифтом или другими специальными способами для слепых правомерно опубликованных произведений, кроме произведений, специально созданных для воспроизведения такими способами.

Лицо, правомерно владеющее экземпляром программы для ЭВМ или экземпляром базы данных (пользователь), вправе без разрешения автора или иного правообладателя и без выплаты дополнительного вознаграждения:

– внести в программу для ЭВМ или базу данных изменения исключительно в целях их функционирования на технических средствах пользователя и осуществлять действия, необходимые для функционирования такой программы или базы данных в соответствии с их назначением, в том числе запись и хранение в памяти

ЭВМ (одной ЭВМ или одного пользователя сети), а также осуществить исправление явных ошибок, если иное не предусмотрено договором с правообладателем;

– изготовить копию программы для ЭВМ или базы данных при условии, что эта копия предназначена только для архивных целей или для замены правомерно приобретенного экземпляра в случаях, когда такой экземпляр утерян, уничтожен или стал непригоден для использования.

Лицо, правомерно владеющее экземпляром программы для ЭВМ, вправе без согласия правообладателя и без выплаты дополнительного вознаграждения:

– изучать, исследовать или испытывать функционирование такой программы в целях определения идей и принципов, лежащих в основе любого элемента программы для ЭВМ, путем осуществления определенных законодательством действий;

– воспроизвести и преобразовать объектный код в исходный текст (декомпилировать программу для ЭВМ) или поручить иным лицам осуществить эти действия, если они необходимы для достижения способности к взаимодействию независимо разработанной этим лицом программы для ЭВМ с другими программами, которые могут взаимодействовать с декомпилируемой программой, при соблюдении следующих условий:

1) информация, необходимая для достижения способности к взаимодействию, ранее не была доступна этому лицу из других источников;

2) указанные действия осуществляются в отношении только тех частей декомпилируемой программы для ЭВМ, которые необходимы для достижения способности к взаимодействию;

3) информация, полученная в результате декомпилирования, может использоваться лишь для достижения способности к взаимодействию независимо разработанной программы для ЭВМ с другими программами, не может передаваться иным лицам, за исключением случаев, когда это необходимо для достижения способности к взаимодействию независимо разработанной программы для ЭВМ с другими программами, а также не может использоваться для разработки программы для ЭВМ, по своему виду существенно схожей с декомпилируемой программой для ЭВМ, или для осуществления другого действия, нарушающего исключительное право на программу для ЭВМ.

Исключительное право на произведение действует в течение всей жизни автора и семидесяти лет, считая с 1 января года, следующего за годом смерти автора.

По истечении срока действия исключительного права произведение науки, литературы или искусства, как обнародованное, так и необнародованное, переходит в *общественное достояние.*

Произведение, перешедшее в общественное достояние, может свободно использоваться любым лицом без чьего-либо согласия или разрешения и без выплаты авторского вознаграждения.

При этом охраняются авторство, имя автора и неприкосновенность произведения.

Смежными с авторскими правами (***смежными правами***) являются интеллектуальные права: на результаты исполнительской деятельности (исполнения), на фонограммы, на сообщение в эфир или по кабелю радио- и телепередач (вещание организаций эфирного и кабельного вещания), на содержание баз данных, на произведения науки, литературы и искусства, впервые обнародованные после их перехода в общественное достояние (право публикатора).

К *смежным правам относятся* исключительное право, а в случаях, предусмотренных настоящим Кодексом, также личные неимущественные права.

Объектами смежных прав являются:

– исполнения артистов-исполнителей и дирижеров, постановки режиссеров — постановщиков спектаклей (исполнения), если эти исполнения выражаются в форме, допускающей их воспроизведение и распространение с помощью технических средств;

– фонограммы, т.е. любые исключительно звуковые записи исполнений или иных звуков либо их отображений, за исключением звуковой записи, включенной в аудиовизуальное произведение;

– сообщения передач организаций эфирного или кабельного вещания, в том числе передач, созданных самой организацией эфирного или кабельного вещания либо по ее заказу за счет ее средств другой организацией;

– базы данных в части их охраны от несанкционированного извлечения и повторного использования составляющих их содержание материалов;

– произведения науки, литературы и искусства, обнародованные после их перехода в общественное достояние, в части охраны прав публикаторов таких произведений.

Для возникновения, осуществления и защиты смежных прав не требуются регистрация их объекта или соблюдение каких-либо иных формальностей.

Исполнителем (*автором исполнения*) признается гражданин, творческим трудом которого создано исполнение, — артист-исполнитель (актер, певец, музыкант, танцор или другое лицо, которое играет роль, читает, декламирует, поет, играет на музыкальном инструменте или иным образом участвует в исполнении произведения литературы, искусства или народного творчества, в том числе эстрадного, циркового или кукольного номера), а также режиссер-постановщик спектакля (лицо, осуществившее постановку театрального, циркового, кукольного, эстрадного или иного театрально-зрелищного представления) и дирижер.

Исполнителю принадлежат:

– исключительное право на исполнение;

– право авторства — право признаваться автором исполнения;

– право на имя — право на указание своего имени или псевдонима на экземплярах фонограммы и в иных случаях использования исполнения, а в случае, предусмотренном законодательством, право на указание наименования коллектива исполнителей, кроме случаев, когда характер использования произведения исключает возможность указания имени исполнителя или наименования коллектива исполнителей;

– право на неприкосновенность исполнения — право на защиту исполнения от всякого искажения, т.е. от внесения в запись, в сообщение в эфир или по кабелю изменений, приводящих к извращению смысла или к нарушению целостности восприятия исполнения.

Исключительное право на исполнение — возможность правообладателя исполнять любым не противоречащим закону способом, а также распоряжаться исключительным правом на исполнение.

Использованием исполнения считается:

– сообщение в эфир, т.е. сообщение исполнения для всеобщего сведения посредством его передачи по радио или телевидению (в том числе путем ретрансляции), за исключением кабельного телевидения (под сообщением понимается любое действие, посредством которого исполнение становится доступным для слухового и (или) зрительного восприятия независимо от его фактического восприятия публикой; при сообщении исполнения в эфир через спутник под сообщением в эфир понимается прием сигналов с наземной станции на спутник и передача сигналов со спутника, посредством которых исполнение может быть доведено до всеобщего сведения независимо от его фактического приема публикой);

– сообщение по кабелю, т.е. сообщение исполнения для всеобщего сведения посредством его передачи по радио или телевидению с помощью кабеля, провода, оптического волокна или аналогичных средств (в том числе путем ретрансляции);

– запись исполнения, т.е. фиксация звуков и (или) изображения или их отображений с помощью технических средств в какой-либо материальной форме, позволяющей осуществлять их неоднократное восприятие, воспроизведение или сообщение;

– воспроизведение записи исполнения, т.е. изготовление одного и более экземпляра фонограммы либо ее части. При этом запись исполнения на электронном носителе, в том числе запись в память ЭВМ, также считается воспроизведением, кроме случаев, когда такая запись является временной и составляет неотъемлемую и существенную часть технологического процесса, имеющего единственной целью правомерное использование записи или правомерное доведение исполнения до всеобщего сведения;

– распространение записи исполнения путем продажи или иного отчуждения ее оригинала или экземпляров, представляющих собой копии такой записи на любом материальном носителе;

– действие, осуществляемое в отношении записи исполнения и предусмотренное законодательством;

– доведение записи исполнения до всеобщего сведения таким образом, что любое лицо может получить доступ к записи исполнения из любого места и в любое время по собственному выбору (доведение до всеобщего сведения);

– публичное исполнение записи исполнения, т.е. любое сообщение записи с помощью технических средств в месте, открытом для свободного посещения, или в месте, где присутствует значительное число лиц, не принадлежащих к обычному кругу семьи, независимо от того, воспринимается запись в месте ее сообщения или в другом месте одновременно с ее сообщением;

– прокат оригинала или экземпляров записи исполнения.

Изготовителем фонограммы признается лицо, взявшее на себя инициативу и ответственность за первую запись звуков исполнения или других звуков либо отображений этих звуков. При отсутствии доказательств иного изготовителем фонограммы признается лицо, имя или наименование которого указано обычным образом на экземпляре фонограммы и (или) его упаковке.

Изготовителю фонограммы принадлежат:

– исключительное право на фонограмму;

– право на указание на экземплярах фонограммы и (или) их упаковке своего имени или наименования;

– право на защиту фонограммы от искажения при ее использовании;

– право на обнародование фонограммы, т.е. на осуществление действия, которое впервые делает фонограмму доступной для всеобщего сведения путем ее опубликования, публичного показа, публичного исполнения, сообщения в эфир или по кабелю либо иным способом. При этом опубликованием (выпуском в свет) является выпуск в обращение экземпляров фонограммы с согласия изготовителя в количестве, достаточном для удовлетворения разумных потребностей публики.

Исключительное право изготовителя фонограммы заключается в возможности использовать фонограмму любым не противоречащим закону способом, а также распоряжаться этим исключительным правом.

Использованием фонограммы считается:

– публичное исполнение, т.е. любое сообщение фонограммы с помощью технических средств в месте, открытом для свободного посещения, или в месте, где присутствует значительное число лиц, не принадлежащих к обычному кругу семьи, независимо от

того, воспринимается фонограмма в месте ее сообщения или в другом месте одновременно с ее сообщением;

– сообщение в эфир, т.е. сообщение фонограммы для всеобщего сведения посредством ее передачи по радио или телевидению (в том числе путем ретрансляции), за исключением сообщения по кабелю. При этом под сообщением понимается любое действие, посредством которого фонограмма становится доступной для слухового восприятия независимо от ее фактического восприятия публикой. Под сообщением фонограммы в эфир через спутник понимается прием сигналов с наземной станции на спутник и передача сигналов со спутника, посредством которых фонограмма может быть доведена до всеобщего сведения независимо от ее фактического приема публикой;

– сообщение по кабелю, т.е. сообщение фонограммы для всеобщего сведения посредством ее передачи по радио или телевидению с помощью кабеля, провода, оптического волокна или аналогичных средств (в том числе путем ретрансляции);

– доведение фонограммы до всеобщего сведения таким образом, что лицо может получить доступ к фонограмме из любого места и в любое время по собственному выбору (доведение до всеобщего сведения);

– воспроизведение, т.е. изготовление одного и более экземпляра фонограммы или части фонограммы. При этом запись фонограммы или части фонограммы на электронном носителе, в том числе запись в память ЭВМ, также считается воспроизведением, кроме случая, когда такая запись является временной и составляет неотъемлемую и существенную часть технологического процесса, имеющего единственной целью правомерное использование записи или правомерное доведение фонограммы до всеобщего сведения;

– распространение фонограммы путем продажи или иного отчуждения оригинала или экземпляров, представляющих собой копию фонограммы на любом материальном носителе;

– импорт оригинала или экземпляров фонограммы в целях распространения, включая экземпляры, изготовленные с разрешения правообладателя;

– прокат оригинала и экземпляров фонограммы;

– переработка фонограммы.

Право на указание на экземплярах фонограммы и (или) их упаковке своего имени или наименования и право на защиту фонограммы от искажения действуют и охраняются в течение всей жизни гражданина либо до прекращения юридического лица, являющегося изготовителем фонограммы.

Организациям эфирного или кабельного вещания принадлежит *исключительное право на сообщение радио- или телепередачи*, которое заключается в возможности использовать правомерно осуществляемое или осуществленное ими сообщение в эфир или по

кабелю передач любым не противоречащим закону способом, а также возможности распоряжаться исключительным правом на сообщение радио- или телепередачи.

Организацией эфирного или кабельного вещания признается юридическое лицо, осуществляющее сообщение в эфир или по кабелю радио- или телепередач (совокупности звуков и (или) изображений или их отображений).

Изготовителем базы данных признается лицо, организовавшее создание базы данных и работу по сбору, обработке и расположению составляющих ее материалов. При отсутствии доказательств иного изготовителем базы данных признается гражданин или юридическое лицо, имя или наименование которых указано обычным образом на экземпляре базы данных и (или) его упаковке.

Изготовителю базы данных принадлежат:

– исключительное право изготовителя базы данных;

– право на указание на экземплярах базы данных и (или) их упаковках своего имени или наименования.

Исключительное право изготовителя базы данных, создание которой (включая обработку или представление соответствующих материалов) требует существенных финансовых, материальных, организационных или иных затрат, заключается в возможности извлекать из базы данных материалы и осуществлять их последующее использование в любой форме и любым способом, не противоречащим законодательству, а также распоряжаться указанным исключительным правом.

При отсутствии доказательств иного базой данных, создание которой требует существенных затрат, признается база данных, содержащая не менее десяти тысяч самостоятельных информационных элементов (материалов), составляющих содержание базы данных.

Никто не вправе извлекать из базы данных материалы и осуществлять их последующее использование без разрешения правообладателя, кроме случаев, предусмотренных законодательством (под извлечением материалов понимается перенос всего содержания базы данных или существенной части составляющих ее материалов на другой информационный носитель с использованием любых технических средств и в любой форме).

Права публикатора распространяются на произведения, которые независимо от времени их создания могли быть признаны объектами авторского права в соответствии с законодательством.

Публикатором признается гражданин, который правомерно обнародовал или организовал обнародование произведения науки, литературы или искусства, ранее не обнародованного и перешедшего в общественное достояние либо находящегося в общественном достоянии в силу того, что оно не охранялось авторским правом.

Публикатору принадлежат:

– исключительное право публикатора на обнародованное им произведение;

– право на указание своего имени на экземплярах обнародованного им произведения и в иных случаях его использования, в том числе при переводе или другой переработке произведения.

Исключительное право публикатора на произведение заключается в возможности использовать произведение способами, предусмотренными законодательством, а также распоряжаться указанным исключительным правом.

9.3. Патентное право

Патентными правами являются интеллектуальные права на изобретения, полезные модели, промышленные образцы.

Автору изобретения, полезной модели или *промышленного образца* принадлежат исключительное право, право авторства.

В случаях, предусмотренных законодательством, автору изобретения, полезной модели или промышленного образца принадлежат также другие права, в том числе право на получение патента, право на вознаграждение за использование служебного изобретения, полезной модели или промышленного образца.

Автором изобретения, полезной модели или промышленного образца признается гражданин, творческим трудом которого создан соответствующий результат интеллектуальной деятельности. Лицо, указанное в качестве автора в заявке на выдачу патента на изобретение, полезную модель или промышленный образец, считается автором изобретения, полезной модели или промышленного образца, если не доказано иное.

Объектами патентных прав являются результаты интеллектуальной деятельности в научно-технической сфере, отвечающие установленным законодательством требованиям к изобретениям и полезным моделям, и результаты интеллектуальной деятельности в сфере художественного конструирования, отвечающие установленным требованиям к промышленным образцам.

Не могут быть объектами патентных прав способы клонирования человека, способы модификации генетической целостности клеток зародышевой линии человека, использование человеческих эмбрионов в промышленных и коммерческих целях, иные решения, противоречащие общественным интересам, принципам гуманности и морали.

В качестве изобретения охраняется техническое решение в любой области, относящееся к продукту (в частности, устройству, веществу, штамму микроорганизма, культуре клеток растений или животных) или способу (процессу осуществления действий над материальным объектом с помощью материальных средств).

Изобретению предоставляется правовая охрана, если оно является новым — совокупность его существенных признаков не известно из уровня техники; имеет изобретательский уровень — для специалиста явным образом не следует из уровня техники; промышленно применимо — может быть использовано в промышленности, сельском хозяйстве, здравоохранении, других отраслях экономики или в социальной сфере.

Раскрытие информации, относящейся к изобретению, автором изобретения, заявителем или любым лицом, получившим от них прямо или косвенно эту информацию, в результате чего сведения о сущности изобретения стали общедоступными, не является обстоятельством, препятствующим признанию патентоспособности изобретения, при условии, что заявка на выдачу патента на изобретение подана в федеральный орган исполнительной власти по интеллектуальной собственности в течение шести месяцев со дня раскрытия информации. Бремя доказывания того, что обстоятельства, в силу которых раскрытие информации не препятствует признанию патентоспособности изобретения, имели место, лежит на заявителе.

Не являются изобретениями: открытия; научные теории и математические методы; решения, касающиеся только внешнего вида изделий и направленные на удовлетворение эстетических потребностей; правила и методы игр, интеллектуальной или хозяйственной деятельности; программы для ЭВМ; решения, заключающиеся только в представлении информации.

Не предоставляется правовая охрана в качестве изобретения сортам растений, породам животных и биологическим способам их получения, за исключением микробиологических способов и продуктов, полученных такими способами; топологиям интегральных микросхем.

В качестве полезной модели охраняется техническое решение, относящееся к устройству.

Полезной модели предоставляется правовая охрана, если она является новой — совокупность ее существенных признаков не известна из уровня техники; промышленно применимой — может быть использована в промышленности, сельском хозяйстве, здравоохранении, других отраслях экономики или в социальной сфере.

Раскрытие информации, относящейся к полезной модели, автором полезной модели, заявителем или любым лицом, получившим от них прямо или косвенно эту информацию, в результате чего сведения о сущности полезной модели стали общедоступными, не является обстоятельством, препятствующим признанию патентоспособности полезной модели, при условии, что заявка на выдачу патента на полезную модель подана в федеральный орган исполнительной власти по интеллектуальной собственности в течение шести месяцев со дня раскрытия информации. Бремя дока-

зывания того, что обстоятельства, в силу которых раскрытие информации не препятствует признанию патентоспособности полезной модели, имели место, лежит на заявителе.

Не предоставляется правовая охрана в качестве полезной модели: решениям, касающимся только внешнего вида изделий и направленным на удовлетворение эстетических потребностей; топологиям интегральных микросхем

В качестве промышленного образца охраняется художественно-конструкторское решение изделия промышленного или кустарно-ремесленного производства, определяющее его внешний вид.

Промышленному образцу предоставляется правовая охрана, если по своим существенным признакам он является: новым — совокупность его существенных признаков, нашедших отражение на изображениях изделия и приведенных в перечне существенных признаков промышленного образца (к существенным признакам промышленного образца относятся признаки, определяющие эстетические и (или) эргономические особенности внешнего вида изделия, в частности форма, конфигурация, орнамент и сочетание цветов) не известна из сведений, ставших общедоступными в мире до даты приоритета промышленного образца; оригинальным — его существенные признаки обусловлены творческим характером особенностей изделия.

Раскрытие информации, относящейся к промышленному образцу, автором промышленного образца, заявителем или любым лицом, получившим от них прямо или косвенно эту информацию, в результате чего сведения о сущности промышленного образца стали общедоступными, не является обстоятельством, препятствующим признанию патентоспособности промышленного образца, при условии, что заявка на выдачу патента на промышленный образец подана в федеральный орган исполнительной власти по интеллектуальной собственности в течение шести месяцев со дня раскрытия информации. Бремя доказывания того, что обстоятельства, в силу которых раскрытие информации не препятствует признанию патентоспособности промышленного образца, имели место, лежит на заявителе.

Не предоставляется правовая охрана в качестве промышленного образца: решениям, обусловленным исключительно технической функцией изделия; объектам архитектуры (кроме малых архитектурных форм), промышленным, гидротехническим и другим стационарным сооружениям; объектам неустойчивой формы из жидких, газообразных, сыпучих или им подобных веществ.

Исключительное право на изобретение, полезную модель или промышленный образец признается и охраняется при условии государственной регистрации соответствующих изобретения, полезной модели или промышленного образца, на основании которой федеральный орган исполнительной власти по интеллектуальной

собственности выдает патент на изобретение, полезную модель или промышленный образец.

Патент на изобретение, полезную модель или промышленный образец удостоверяет приоритет изобретения, полезной модели или промышленного образца, авторство и исключительное право на изобретение, полезную модель или промышленный образец.

Охрана интеллектуальных прав на изобретение или полезную модель предоставляется на основании патента в объеме, определяемом содержащейся в патенте формулой изобретения или соответственно полезной модели. Для толкования формулы изобретения и формулы полезной модели могут использоваться описание и чертежи.

Охрана интеллектуальных прав на промышленный образец предоставляется на основании патента в объеме, определяемом совокупностью его существенных признаков, нашедших отражение на изображениях изделия и приведенных в перечне существенных признаков промышленного образца.

Патентные права включают: право авторства на изобретение, полезную модель или промышленный образец; право на получение патента на изобретение, полезную модель или промышленный образец; исключительное право на изобретение, полезную модель или промышленный образец.

Право авторства, т.е. право признаваться автором изобретения, полезной модели или промышленного образца, неотчуждаемо и непередаваемо, в том числе при передаче другому лицу или переходе к нему исключительного права на изобретение, полезную модель или промышленный образец и при предоставлении другому лицу права его использования.

Право на получение патента на изобретение, полезную модель или промышленный образец первоначально принадлежит автору изобретения, полезной модели или промышленного образца. Это право может перейти к другому лицу (правопреемнику) или быть ему передано в случаях и по основаниям, которые установлены законом, в том числе в порядке универсального правопреемства, или по договору, в том числе по трудовому договору.

Исключительное право использования изобретения, полезной модели или промышленного образца принадлежит патентообладателю и заключается в возможности использовать эти объекты любым не противоречащим закону способом, а также распоряжаться исключительным правом на изобретение, полезную модель или промышленный образец.

Использованием изобретения, полезной модели или промышленного образца считается, в частности:

– ввоз на территорию Российской Федерации, изготовление, применение, предложение о продаже, продажа, иное введение в гражданский оборот или хранение для этих целей продукта, в

котором использованы изобретение или полезная модель, либо изделия, в котором использован промышленный образец;

– совершение действий, предусмотренных предыдущим абзацем, в отношении продукта, полученного непосредственно запатентованным способом. Если продукт, получаемый запатентованным способом, является новым, идентичный продукт считается полученным путем использования запатентованного способа, поскольку не доказано иное;

– совершение аналогичных действий в отношении устройства, при функционировании (эксплуатации) которого в соответствии с его назначением автоматически осуществляется запатентованный способ;

– осуществление способа, в котором используется изобретение, в частности, путем применения этого способа.

Изобретение или полезная модель признаются использованными в продукте или способе, если продукт содержит, а в способе использован каждый признак изобретения или полезной модели, приведенный в независимом пункте содержащейся в патенте формулы изобретения или полезной модели, либо признак, эквивалентный ему и ставший известным в качестве такового в данной области техники до совершения в отношении соответствующего продукта или способа действий, предусмотренных законодательством.

9.4. Право на топологии интегральных микросхем

Топологией интегральной микросхемы является зафиксированное на материальном носителе пространственно-геометрическое расположение совокупности элементов интегральной микросхемы и связей между ними. *Интегральной микросхемой* является микроэлектронное изделие окончательной или промежуточной формы, которое предназначено для выполнения функций электронной схемы, элементы и связи которого нераздельно сформированы в объеме и (или) на поверхности материала, на основе которого изготовлено такое изделие.

Правовая охрана, предоставляемая законодательством, распространяется только на оригинальную (пока не доказано обратное) топологию интегральной микросхемы, созданную в результате творческой деятельности автора и неизвестную автору и (или) специалистам в области разработки топологий интегральных микросхем на дату ее создания. Топологии интегральной микросхемы, состоящей из элементов, которые известны специалистам в области разработки топологий интегральных микросхем на дату ее создания, предоставляется правовая охрана, если совокупность таких элементов в целом отвечает требованию оригинальности.

Правовая охрана не распространяется на идеи, способы, системы, технологию или закодированную информацию, которые могут быть воплощены в топологии интегральной микросхемы.

Автору топологии интегральной микросхемы, отвечающей условиям предоставления правовой охраны, предусмотренным законодательством (топологии), принадлежат исключительное право, право авторства, другие права, в том числе право на вознаграждение за использование служебной топологии в случаях, предусмотренных законодательством.

Автором топологии интегральной микросхемы признается гражданин, творческим трудом которого создана такая топология. Лицо, указанное в качестве автора в заявке на выдачу свидетельства о государственной регистрации топологии интегральной микросхемы, считается автором этой топологии, если не доказано иное.

Исключительное право использования топологии заключается в возможности правообладателя использовать этот объект интеллектуальной собственности любым не противоречащим закону способом (исключительное право на топологию), а также распоряжаться исключительным правом на топологию.

Использованием топологии признаются действия, направленные на извлечение прибыли, в частности:

– воспроизведение топологии в целом или частично путем включения в интегральную микросхему либо иным образом, за исключением воспроизведения только той части топологии, которая не является оригинальной;

– ввоз на территорию Российской Федерации, продажа и иное введение в гражданский оборот топологии или интегральной микросхемы, в которую включена эта топология, или изделия, включающего такую интегральную микросхему.

За лицом, независимо создавшим топологию, идентичную другой топологии, признается самостоятельное исключительное право на эту топологию.

9.5. Право на секрет производства (ноу-хау)

Секретом производства (*ноу-хау*) признаются сведения любого характера (производственные, технические, экономические, организационные и другие), в том числе о результатах интеллектуальной деятельности в научно-технической сфере, а также сведения о способах осуществления профессиональной деятельности, которые имеют действительную или потенциальную коммерческую ценность в силу неизвестности их третьим лицам, к которым у третьих лиц нет свободного доступа на законном основании и в отношении которых обладателем таких сведений введен режим коммерческой тайны.

Исключительное право использования секрета производства принадлежит его обладателю и заключается в возможности его использования любым не противоречащим закону способом, в том числе при изготовлении изделий и реализации экономических и организационных решений, а также в возможности распоряжаться указанным исключительным правом.

Лицо, ставшее добросовестно и независимо от других обладателей секрета производства обладателем сведений, составляющих содержание охраняемого секрета производства, приобретает самостоятельное исключительное право на этот секрет производства.

Исключительное право на секрет производства действует до тех пор, пока сохраняется конфиденциальность сведений, составляющих его содержание. С момента утраты конфиденциальности соответствующих сведений исключительное право на секрет производства прекращается у всех правообладателей.

9.6. Право на средства индивидуализации юридических лиц, товаров, работ, услуг и предприятий

Право на средства индивидуализации юридических лиц, товаров, работ, услуг и предприятий включает: право на фирменное наименование; право на товарный знак; право на знак обслуживания; право на наименование места происхождения товара; право на коммерческое обозначение.

Право на фирменное наименование — исключительное право юридического лица, являющегося коммерческой организацией, на использование в гражданском обороте своего фирменного наименования в качестве средства индивидуализации любым не противоречащим закону способом (исключительное право на фирменное наименование), в том числе путем его указания на вывесках, бланках, в счетах и иной документации, в объявлениях и рекламе, на товарах или их упаковках.

Фирменное наименование определяется в учредительных документах и включается в единый государственный реестр юридических лиц при государственной регистрации юридического лица.

Сокращенные фирменные наименования, а также фирменные наименования на языках народов Российской Федерации и иностранных языках защищаются исключительным правом на фирменное наименование при условии их включения в единый государственный реестр юридических лиц.

Распоряжение исключительным правом на фирменное наименование (в том числе путем его отчуждения или предоставления другому лицу права использования фирменного наименования) не допускается.

Не допускается использование юридическим лицом фирменного наименования, тождественного фирменному наименованию

другого юридического лица или сходного с ним до степени смешения, если указанные юридические лица осуществляют аналогичную деятельность и фирменное наименование второго юридического лица было включено в единый государственный реестр юридических лиц ранее, чем фирменное наименование первого юридического лица.

Фирменное наименование или отдельные его элементы могут использоваться правообладателем в составе принадлежащего ему коммерческого обозначения, товарном знаке и знаке обслуживания.

Право на товарный знак заключается в исключительном праве использования правообладателями (юридическими лицами и предпринимателями, на имя которых зарегистрирован товарный знак) данного средства индивидуализации любым не противоречащим закону способом, а также в возможности распоряжаться исключительным правом на товарный знак.

Товарный знак — обозначение, служащее для индивидуализации товаров юридических лиц или индивидуальных предпринимателей.

Исключительное право на товарный знак может быть осуществлено для индивидуализации товаров, работ или услуг, в отношении которых товарный знак зарегистрирован, в частности, путем размещения товарного знака:

– на товарах, в том числе на этикетках, упаковках товаров, которые производятся, предлагаются к продаже, продаются, демонстрируются на выставках и ярмарках или иным образом вводятся в гражданский оборот на территории Российской Федерации, либо хранятся или перевозятся с этой целью, либо ввозятся на территорию Российской Федерации;

– при выполнении работ, оказании услуг;

– на документации, связанной с введением товаров в гражданский оборот;

– в предложениях о продаже товаров, о выполнении работ, об оказании услуг, а также в объявлениях, на вывесках и в рекламе;

– в сети Интернет, в том числе в доменном имени и при других способах адресации.

Никто не вправе использовать без разрешения правообладателя сходные с его товарным знаком обозначения в отношении товаров, для индивидуализации которых товарный знак зарегистрирован, или однородных товаров, если в результате такого использования возникнет вероятность смешения.

Государственная регистрация товарного знака осуществляется федеральным органом исполнительной власти по интеллектуальной собственности в Государственном реестре товарных знаков и знаков обслуживания Российской Федерации (Государственный реестр товарных знаков) в порядке, установленном законодательством.

К *знакам обслуживания*, т.е. к обозначениям, служащим для индивидуализации выполняемых юридическими лицами либо индивидуальными предпринимателями работ или оказываемых ими услуг, применяются нормы законодательства о товарных знаках.

Право на наименование места происхождения товара заключается в исключительном праве использования правообладателем наименования места происхождения товара, зарегистрированном федеральным органом исполнительной власти по интеллектуальной собственности, а также в других случаях, предусмотренных международным договором Российской Федерации, любым не противоречащим закону способом.

Использованием наименования места происхождения товара считается размещение этого наименования, в частности:

– на товарах, этикетках, упаковках товаров, которые производятся, предлагаются к продаже, продаются, демонстрируются на выставках и ярмарках или иным образом вводятся в гражданский оборот на территории Российской Федерации, либо хранятся или перевозятся с этой целью, либо ввозятся на территорию Российской Федерации;

– на бланках, счетах, иной документации и в печатных изданиях, связанных с введением товаров в гражданский оборот;

– в предложениях о продаже товаров, а также в объявлениях, на вывесках и в рекламе;

– в сети Интернет, в том числе в доменном имени и при других способах адресации.

Наименованием места происхождения товара, которому придается правовая охрана, является обозначение, представляющее собой либо содержащее современное или историческое, официальное или неофициальное, полное или сокращенное наименование страны, городского или сельского поселения, местности или другого географического объекта, а также обозначение, производное от такого наименования и ставшее известным в результате его использования в отношении товара, особые свойства которого исключительно или главным образом определяются характерными для данного географического объекта природными условиями и (или) людскими факторами. На использование этого наименования может быть признано исключительное право производителей такого товара.

Лицам, зарегистрировавшим наименование места происхождения товара, предоставляется исключительное право использования этого наименования, удостоверяемое свидетельством, при условии, что производимый этими лицами товар отвечает требованиям законодательства.

Исключительное право использования наименования места происхождения товара в отношении того же наименования может

быть предоставлено любому лицу, которое в границах того же географического объекта производит товар, обладающий теми же особыми свойствами.

Право на коммерческое обозначение заключается в исключительном праве правообладателя на использование данного средства индивидуализации принадлежащего ему предприятия любым не противоречащим закону способом, в том числе путем указания коммерческого обозначения на вывесках, бланках, в счетах и на иной документации, в объявлениях и рекламе, на товарах или их упаковках, если такое обозначение обладает достаточными различительными признаками и его употребление правообладателем для индивидуализации своего предприятия является известным в пределах определенной территории.

Юридические лица, осуществляющие предпринимательскую деятельность (в том числе некоммерческие организации, которым право на осуществление такой деятельности предоставлено в соответствии с законом их учредительными документами), а также индивидуальные предприниматели могут использовать для индивидуализации принадлежащих им торговых, промышленных и других предприятий коммерческие обозначения, не являющиеся фирменными наименованиями и не подлежащие обязательному включению в учредительные документы и единый государственный реестр юридических лиц.

9.7. Право использования результатов интеллектуальной деятельности в составе единой технологии

Единой технологией признается выраженный в объективной форме результат научно-технической деятельности, который включает в том или ином сочетании изобретения, полезные модели, промышленные образцы, программы для ЭВМ или другие результаты интеллектуальной деятельности, подлежащие правовой охране в соответствии с правилами настоящего раздела, и может служить технологической основой определенной практической деятельности в гражданской или военной сфере (единая технология).

В состав единой технологии могут входить также результаты интеллектуальной деятельности, не подлежащие правовой охране, в том числе технические данные, другая информация.

Исключительные права на результаты интеллектуальной деятельности, которые входят в состав единой технологии, признаются и подлежат защите в соответствии с законодательством.

Право использовать результаты интеллектуальной деятельности в составе единой технологии как в составе сложного объекта принадлежит лицу, организовавшему создание единой технологии (право на технологию) на основании договоров с обладателями

исключительных прав на результаты интеллектуальной деятельности, входящие в состав единой технологии. В состав единой технологии могут входить также охраняемые результаты интеллектуальной деятельности, созданные самим лицом, организовавшим ее создание.

Предметом правового регулирования отношений в области использования результатов интеллектуальной деятельности в составе единой технологии являются отношения, связанные с правом на технологию гражданского, военного, специального или двойного назначения, созданную за счет или с привлечением средств федерального бюджета либо бюджетов субъектов Российской Федерации, выделяемых для оплаты работ по государственным контрактам, по другим договорам, для финансирования по сметам доходов и расходов, а также в виде субсидий.

Указанные правила не применяются к отношениям, возникающим при создании единой технологии за счет или с привлечением средств федерального бюджета либо бюджетов субъектов Российской Федерации на возмездной основе в форме бюджетного кредита.

Лицу, организовавшему создание единой технологии за счет или с привлечением средств федерального бюджета или бюджета субъекта Российской Федерации (*исполнителю*), принадлежит право на созданную технологию, за исключением случаев, когда это право в соответствии с законодательством принадлежит Российской Федерации или субъекту Российской Федерации.

Лицо, которому принадлежит право на технологию, обязано незамедлительно принимать предусмотренные законодательством Российской Федерации меры для признания за ним и получения прав на результаты интеллектуальной деятельности, входящие в состав единой технологии (подавать заявки на выдачу патентов, на государственную регистрацию результатов интеллектуальной деятельности, вводить в отношении соответствующей информации режим сохранения тайны, заключать договоры об отчуждении исключительных прав и лицензионные договоры с обладателями исключительных прав на соответствующие результаты интеллектуальной деятельности, входящие в состав единой технологии, и принимать иные меры), если такие меры не были приняты до или в процессе создания технологии.

В случаях, когда законодательство допускает различные способы правовой охраны результатов интеллектуальной деятельности, входящих в состав единой технологии, лицо, которому принадлежит право на технологию, выбирает тот способ правовой охраны, который в наибольшей степени соответствует его интересам и обеспечивает практическое применение единой технологии.

Лицо, которому принадлежит право на технологию, обязано осуществлять ее практическое применение (внедрение).

Содержание обязанности внедрения технологии, сроки, другие условия и порядок исполнения этой обязанности, последствия ее неисполнения и условия прекращения определяются Правительством Российской Федерации.

Контрольные вопросы

1. Раскройте содержание понятия «интеллектуальная собственность».
2. Расскажите содержание предмета и механизм действия авторского права и смежных прав.
3. Каковы основные отличия патентного права от авторского права?
4. Что такое «средства индивидуализации» и какова цель их правовой защиты?
5. Раскройте содержание права на топологию интегральных микросхем.
6. Изложите содержание права на секрет производства.
7. Раскройте содержание права на использование результатов интеллектуальной деятельности в составе единой технологии.

Глава 10

ЗАКОНОДАТЕЛЬСТВО О КОММЕРЧЕСКОЙ ТАЙНЕ

10.1. Общие положения

Законодательство Российской Федерации о коммерческой тайне состоит из Гражданского кодекса Российской Федерации, Федерального закона «О коммерческой тайне» и других федеральных законов.

Предмет правового регулирования составляют отношения, связанные с отнесением информации к коммерческой тайне, передачей такой информации, охраной ее конфиденциальности в целях обеспечения баланса интересов обладателей информации, составляющей коммерческую тайну, и других участников регулируемых отношений, в том числе государства, на рынке товаров, работ, услуг и предупреждения недобросовестной конкуренции.

В законодательстве под ***коммерческой тайной*** понимается конфиденциальность информации, позволяющая ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду.

Режим коммерческой тайны образуется совокупностью правовых, организационных, технических и иных принимаемых обладателем информации, составляющей коммерческую тайну, мер по охране ее конфиденциальности.

Цель правового регулирования заключается в защите права человека и гражданина на добросовестную конкуренцию, использование своих интеллектуальных способностей.

В основу правового механизма регулирования рассматриваемых отношений положен ***правовой режим коммерческой тайны***, включающий: порядок отнесения информации к коммерческой тайне; порядок охраны; порядок представления.

10.2. Порядок отнесения информации к коммерческой тайне

Порядок отнесения информации к коммерческой тайне определяет:

– объект, в отношении которого может быть установлен правовой режим коммерческой тайны;

– способ установления правового режима коммерческой тайны;

– субъекта коммерческой тайны, уполномоченного устанавливать данный правовой режим коммерческой тайны.

Объектом правового режима коммерческой тайны является научно-техническая, технологическая, производственная, финансово-экономическая или иная информация (в том числе составляющая секреты производства — ноу-хау), которая имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к которой нет свободного доступа на законном основании и в отношении которой обладателем такой информации введен режим коммерческой тайны.

Информация, самостоятельно полученная лицом при осуществлении исследований, систематических наблюдений или иной деятельности, считается полученной законным способом, несмотря на то что содержание указанной информации может совпадать с содержанием информации, составляющей коммерческую тайну, обладателем которой является другое лицо.

Информация, составляющая коммерческую тайну, полученная от ее обладателя на основании договора или на другом законном основании, считается полученной законным способом.

Информация, составляющая коммерческую тайну, обладателем которой является другое лицо, считается полученной незаконно, если ее получение осуществлялось с умышленным преодолением принятых обладателем информации, составляющей коммерческую тайну, мер по охране конфиденциальности этой информации, а также если получающее эту информацию лицо знало или имело достаточные основания полагать, что эта информация составляет коммерческую тайну, обладателем которой является другое лицо, и что осуществляющее передачу этой информации лицо не имеет на передачу этой информации законного основания.

Режим коммерческой тайны не может быть установлен лицами, осуществляющими предпринимательскую деятельность, в отношении следующих сведений:

– содержащихся в учредительных документах юридического лица, документах, подтверждающих факт внесения записей о юридических лицах и об индивидуальных предпринимателях в соответствующие государственные реестры;

– содержащихся в документах, дающих право на осуществление предпринимательской деятельности;

– о составе имущества государственного или муниципального унитарного предприятия, государственного учреждения и об использовании ими средств соответствующих бюджетов;

– о загрязнении окружающей среды, состоянии противопожарной безопасности, санитарно-эпидемиологической и радиационной обстановке, безопасности пищевых продуктов и других факторах, оказывающих негативное воздействие на обеспечение

безопасного функционирования производственных объектов, безопасности каждого гражданина и безопасности населения в целом;

– о численности и составе работников, о системе оплаты труда, об условиях труда, в том числе об охране труда, показателях производственного травматизма и профессиональной заболеваемости, о наличии свободных рабочих мест;

– о задолженности работодателей по выплате заработной платы и иным социальным выплатам;

– о нарушениях законодательства Российской Федерации и фактах привлечения к ответственности за совершение этих нарушений;

– об условиях конкурсов или аукционов по приватизации объектов государственной или муниципальной собственности;

– о размерах и структуре доходов некоммерческих организаций, о размерах и составе их имущества, об их расходах, о численности и оплате труда их работников, об использовании безвозмездного труда граждан в деятельности некоммерческой организации;

– о перечне лиц, имеющих право действовать без доверенности от имени юридического лица;

– обязательность раскрытия которых или недопустимость ограничения доступа к которым установлена иными федеральными законами.

Способ установления режима коммерческой тайны состоит в реализации системы мер по охране конфиденциальности информации, принимаемых ее обладателем, которая должна включать:

– определение перечня информации, составляющей коммерческую тайну;

– ограничение доступа к информации, составляющей коммерческую тайну, путем установления порядка обращения с этой информацией и контроля за соблюдением такого порядка;

– учет лиц, получивших доступ к информации, составляющей коммерческую тайну, и (или) лиц, которым такая информация была предоставлена или передана;

– регулирование отношений по использованию информации, составляющей коммерческую тайну, работниками на основании трудовых договоров и контрагентами на основании гражданско-правовых договоров;

– нанесение на материальные носители (документы), содержащие информацию, составляющую коммерческую тайну, грифа «Коммерческая тайна» с указанием обладателя этой информации (для юридических лиц — полное наименование и место нахождения, для индивидуальных предпринимателей — фамилия, имя, отчество гражданина, являющегося индивидуальным предпринимателем, и место жительства).

Режим коммерческой тайны считается установленным после принятия обладателем информации, составляющей коммерческую тайну, данных мер.

Индивидуальный предприниматель, являющийся обладателем информации, составляющей коммерческую тайну, и не имеющий работников, с которыми заключены трудовые договоры, принимая перечисленные выше меры по охране конфиденциальности информации, может не определять перечень информации, составляющей коммерческую тайну, не устанавливать ограничение доступа к информации, составляющей коммерческую тайну.

Наряду с указанными мерами обладатель информации, составляющей коммерческую тайну, вправе применять при необходимости средства и методы технической защиты конфиденциальности этой информации, другие не противоречащие законодательству Российской Федерации меры.

Меры по охране конфиденциальности информации признаются разумно достаточными при условии, что:

– исключается доступ к информации, составляющей коммерческую тайну, любых лиц без согласия ее обладателя;

– обеспечивается возможность использования информации, составляющей коммерческую тайну, работниками и передачи ее контрагентам без нарушения режима коммерческой тайны.

Режим коммерческой тайны не может быть использован в целях, противоречащих требованиям защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства.

Основным субъектом коммерческой тайны является обладатель информации, составляющей коммерческую тайну. Под таким обладателем понимается лицо, которое владеет информацией, составляющей коммерческую тайну, на законном основании, которое ограничило доступ к этой информации и установило в отношении ее режим коммерческой тайны.

Обладатель информации, составляющей коммерческую тайну, имеет право:

– устанавливать, изменять и отменять в письменной форме режим коммерческой тайны в соответствии с настоящим Федеральным законом и гражданско-правовым договором;

– использовать информацию, составляющую коммерческую тайну, для собственных нужд в порядке, не противоречащем законодательству Российской Федерации;

– разрешать или запрещать доступ к информации, составляющей коммерческую тайну, определять порядок и условия доступа к этой информации;

– вводить в гражданский оборот информацию, составляющую коммерческую тайну, на основании договоров, предусматрива-

ющих включение в них условий об охране конфиденциальности этой информации;

– требовать от юридических и физических лиц, получивших доступ к информации, составляющей коммерческую тайну, органов государственной власти, иных государственных органов, органов местного самоуправления, которым предоставлена информация, составляющая коммерческую тайну, соблюдения обязанностей по охране ее конфиденциальности;

– требовать от лиц, получивших доступ к информации, составляющей коммерческую тайну, в результате действий, осуществленных случайно или по ошибке, охраны конфиденциальности этой информации;

– защищать в установленном законом порядке свои права в случае разглашения, незаконного получения или незаконного использования третьими лицами информации, составляющей коммерческую тайну, в том числе требовать возмещения убытков, причиненных в связи с нарушением его прав.

Права обладателя информации, составляющей коммерческую тайну, возникают с момента установления им в отношении такой информации режима коммерческой тайны.

Обладателем информации, составляющей коммерческую тайну, полученной в рамках трудовых отношений, является работодатель.

В случае получения работником в связи с выполнением своих трудовых обязанностей или конкретного задания работодателя результата, способного к правовой охране в качестве изобретения, полезной модели, промышленного образца, топологии интегральной микросхемы, программы для электронных вычислительных машин или базы данных, отношения между работником и работодателем регулируются в соответствии с законодательством Российской Федерации об интеллектуальной собственности.

Государственным или муниципальным контрактом на выполнение научно-исследовательских, опытно-конструкторских, технологических или иных работ для государственных или муниципальных нужд должен быть определен объем сведений, признаваемых конфиденциальными, а также должны быть урегулированы вопросы, касающиеся установления в отношении полученной информации режима коммерческой тайны.

10.3. Порядок охраны коммерческой тайны

В целях охраны конфиденциальности информации работодатель обязан:

– ознакомить под расписку работника, доступ которого к информации, составляющей коммерческую тайну, необходим для выполнения им своих трудовых обязанностей, с перечнем инфор-

мации, составляющей коммерческую тайну, обладателями которой являются работодатель и его контрагенты;

– ознакомить под расписку работника с установленным работодателем режимом коммерческой тайны и с мерами ответственности за его нарушение;

– создать работнику необходимые условия для соблюдения им установленного работодателем режима коммерческой тайны.

Доступ работника к информации, составляющей коммерческую тайну, осуществляется с его согласия, если это не предусмотрено его трудовыми обязанностями.

В целях охраны конфиденциальности информации работник обязан:

– выполнять установленный работодателем режим коммерческой тайны;

– не разглашать информацию, составляющую коммерческую тайну, обладателями которой являются работодатель и его контрагенты, и без их согласия не использовать эту информацию в личных целях;

– не разглашать информацию, составляющую коммерческую тайну, обладателями которой являются работодатель и его контрагенты, после прекращения трудового договора в течение срока, предусмотренного соглашением между работником и работодателем, заключенным в период срока действия трудового договора, или в течение трех лет после прекращения трудового договора, если указанное соглашение не заключалось;

– возместить причиненный работодателю ущерб, если работник виновен в разглашении информации, составляющей коммерческую тайну, ставшей ему известной в связи с исполнением им трудовых обязанностей;

– передать работодателю при прекращении или расторжении трудового договора имеющиеся в пользовании работника материальные носители информации, содержащие информацию, составляющую коммерческую тайну.

Работодатель вправе потребовать возмещения причиненных убытков лицом, прекратившим с ним трудовые отношения, в случае, если это лицо виновно в разглашении информации, составляющей коммерческую тайну, доступ к которой это лицо получило в связи с исполнением им трудовых обязанностей, если разглашение такой информации последовало в течение установленного законодательством срока.

Причиненные ущерб либо убытки не возмещаются работником или прекратившим трудовые отношения лицом, если разглашение информации, составляющей коммерческую тайну, явилось следствием непреодолимой силы, крайней необходимости или неисполнения работодателем обязанности по обеспечению режима коммерческой тайны.

Трудовым договором с руководителем организации должны предусматриваться его обязательства по обеспечению охраны конфиденциальности информации, обладателем которой являются организация и ее контрагенты, и ответственность за обеспечение охраны ее конфиденциальности.

Руководитель организации возмещает организации убытки, причиненные его виновными действиями в связи с нарушением законодательства Российской Федерации о коммерческой тайне. При этом убытки определяются в соответствии с гражданским законодательством.

Работник имеет право обжаловать в судебном порядке незаконное установление режима коммерческой тайны в отношении информации, к которой он получил доступ в связи с исполнением им трудовых обязанностей.

Отношения между обладателем информации, составляющей коммерческую тайну, и его контрагентом в части, касающейся охраны конфиденциальности информации, регулируются законодательством и договором.

В договоре должны быть определены условия охраны конфиденциальности информации, в том числе в случае реорганизации или ликвидации одной из сторон договора в соответствии с гражданским законодательством, а также обязанность контрагента по возмещению убытков при разглашении им этой информации вопреки договору.

В случае, если иное не установлено договором между обладателем информации, составляющей коммерческую тайну, и контрагентом, контрагент в соответствии с законодательством Российской Федерации самостоятельно определяет способы защиты информации, составляющей коммерческую тайну, переданной ему по договору.

Контрагент обязан незамедлительно сообщить обладателю информации, составляющей коммерческую тайну, о допущенном контрагентом либо ставшем ему известном факте разглашения или угрозы разглашения, незаконном получении или незаконном использовании информации, составляющей коммерческую тайну, третьими лицами.

Обладатель информации, составляющей коммерческую тайну, переданной им контрагенту, до окончания срока действия договора не может разглашать информацию, составляющую коммерческую тайну, а также в одностороннем порядке прекращать охрану ее конфиденциальности, если иное не установлено договором.

Сторона, не обеспечившая в соответствии с условиями договора охраны конфиденциальности информации, переданной по договору, обязана возместить другой стороне убытки, если иное не предусмотрено договором.

10.4. Порядок предоставления информации, составляющей коммерческую тайну

Обладатель информации, составляющей коммерческую тайну, по мотивированному требованию органа государственной власти, иного государственного органа, органа местного самоуправления предоставляет на безвозмездной основе информацию, составляющую коммерческую тайну. Мотивированное требование должно быть подписано уполномоченным должностным лицом, содержать указание цели и правового основания затребования информации, составляющей коммерческую тайну, и срок предоставления этой информации, если иное не установлено федеральными законами.

В случае отказа обладателя информации, составляющей коммерческую тайну, предоставить ее органу государственной власти, иному государственному органу, органу местного самоуправления данные органы вправе затребовать эту информацию в судебном порядке.

Обладатель информации, составляющей коммерческую тайну, а также органы государственной власти, иные государственные органы, органы местного самоуправления, получившие такую информацию, обязаны предоставить эту информацию по запросу судов, органов прокуратуры, органов предварительного следствия, органов дознания по делам, находящимся в их производстве, в порядке и на основаниях, которые предусмотрены законодательством Российской Федерации.

На документах, предоставляемых указанным органам и содержащих информацию, составляющую коммерческую тайну, должен быть нанесен гриф «Коммерческая тайна» с указанием ее обладателя (для юридических лиц — полное наименование и место нахождения, для индивидуальных предпринимателей — фамилия, имя, отчество гражданина, являющегося индивидуальным предпринимателем, и место жительства).

Органы государственной власти, иные государственные органы, органы местного самоуправления в соответствии с законодательством и иными федеральными законами обязаны создать условия, обеспечивающие охрану конфиденциальности информации, предоставленной им юридическими лицами или индивидуальными предпринимателями.

Должностные лица органов государственной власти, иных государственных органов, органов местного самоуправления, государственные или муниципальные служащие указанных органов без согласия обладателя информации, составляющей коммерческую тайну, не вправе разглашать или передавать другим лицам, органам государственной власти, иным государственным органам, органам местного самоуправления ставшую известной им в силу

выполнения должностных (служебных) обязанностей информацию, составляющую коммерческую тайну, за исключением случаев, предусмотренных законодательством, а также не вправе использовать эту информацию в корыстных или иных личных целях.

В случае нарушения конфиденциальности информации должностными лицами органов государственной власти, иных государственных органов, органов местного самоуправления, государственными и муниципальными служащими указанных органов эти лица несут ответственность в соответствии с законодательством Российской Федерации.

10.5. Ответственность за нарушение законодательства

Нарушение законодательства влечет за собой *дисциплинарную, гражданско-правовую, административную или уголовную ответственность* в соответствии с законодательством Российской Федерации.

Работник, который в связи с исполнением трудовых обязанностей, получил доступ к информации, составляющей коммерческую тайну, обладателями которой являются работодатель и его контрагенты, в случае умышленного или неосторожного разглашения этой информации при отсутствии в действиях такого работника состава преступления несет дисциплинарную ответственность в соответствии с законодательством Российской Федерации.

Органы государственной власти, иные государственные органы, органы местного самоуправления, получившие доступ к информации, составляющей коммерческую тайну, несут перед обладателем информации, составляющей коммерческую тайну, гражданско-правовую ответственность за разглашение или незаконное использование этой информации их должностными лицами, государственными или муниципальными служащими указанных органов, которым она стала известна в связи с выполнением ими должностных (служебных) обязанностей.

Лицо, которое использовало информацию, составляющую коммерческую тайну, и не имело достаточных оснований считать использование данной информации незаконным, в том числе получило доступ к ней в результате случайности или ошибки, не может в соответствии с законодательством быть привлечено к ответственности.

По требованию обладателя информации, составляющей коммерческую тайну, такое лицо обязано принять меры по охране конфиденциальности информации. При отказе такого лица принять указанные меры обладатель информации, составляющей коммерческую тайну, вправе требовать в судебном порядке защиты своих прав.

Невыполнение обладателем информации, составляющей коммерческую тайну, законных требований органов государственной власти, иных государственных органов, органов местного самоуправления о предоставлении им информации, составляющей коммерческую тайну, а равно воспрепятствование получению должностными лицами этих органов указанной информации влечет за собой ответственность в соответствии с законодательством Российской Федерации.

Контрольные вопросы

1. Что такое «коммерческая тайна»?
2. Раскройте содержание прав и обязанностей обладателя информации, составляющей коммерческую тайну.
3. В чем заключается способ установления режима коммерческой тайны?
4. Раскройте порядок охраны коммерческой тайны.
5. В чем заключается порядок предоставления информации, составляющей коммерческую тайну?
6. В чем заключается ответственность за нарушение законодательства?

Глава 11

ЗАКОНОДАТЕЛЬСТВО О ГОСУДАРСТВЕННОЙ ТАЙНЕ

11.1. Общие положения

Законодательство Российской Федерации о государственной тайне включает Закон Российской Федерации «О государственной тайне», а также положения других актов законодательства, регулирующих отношения, связанные с защитой государственной тайны.

Предмет правового регулирования — отношения, связанные с отнесением сведений к государственной тайне, их засекречиванием и рассекречиванием, распоряжением этими сведениями, а также их защитой.

Субъектами права в области государственной тайны являются органы законодательной, исполнительной и судебной властей (далее — органы государственной власти), местного самоуправления, предприятия, учреждения и организации независимо от их организационно-правовой формы и формы собственности, должностные лица и граждане Российской Федерации, взявшие на себя обязательства либо обязанные по своему статусу исполнять требования законодательства Российской Федерации о государственной тайне.

Цель правового регулирования заключается в противодействии угрозам несанкционированного раскрытия сведений, составляющих государственную тайну.

Правовой режим государственной тайны включает: порядок отнесения сведений к государственной тайне; порядок засекречивания и рассекречивания; порядок распоряжения сведениями, составляющими государственную тайну; систему защиты сведений, составляющих государственную тайну.

Объект правового режима государственной тайны — защищаемые государством сведения в области военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации.

11.2 Порядок отнесения сведений к государственной тайне

Отнесение сведений к государственной тайне осуществляется уполномоченными субъектами в соответствии с закрепленным в законодательстве перечнем таких сведений.

Государственную тайну составляют:

1. *Сведения в военной области*:

– о содержании стратегических и оперативных планов, документов боевого управления по подготовке и проведению операций, стратегическому, оперативному и мобилизационному развертыванию Вооруженных Сил Российской Федерации, других войск Российской Федерации, воинских формирований и органов, предусмотренных Федеральным законом «Об обороне», их боевой и мобилизационной готовности, о создании и использовании мобилизационных ресурсов;

– планах строительства Вооруженных Сил Российской Федерации, других войск Российской Федерации, направлениях развития вооружения и военной техники, содержании и результатах выполнения целевых программ, научно-исследовательских и опытно-конструкторских работ по созданию и модернизации образцов вооружения и военной техники;

– разработке, технологии, производстве, об объемах производства, хранении, утилизации ядерных боеприпасов, их составных частей, делящихся ядерных материалов, используемых в ядерных боеприпасах, о технических средствах и (или) методах защиты ядерных боеприпасов от несанкционированного применения, а также о ядерных энергетических и специальных физических установках оборонного значения;

– тактико-технических характеристиках и возможностях боевого применения образцов вооружения и военной техники, свойствах, рецептурах или технологиях производства новых видов ракетного топлива или взрывчатых веществ военного назначения;

– дислокации, назначении, степени готовности, защищенности режимных и особо важных объектов, об их проектировании, строительстве и эксплуатации, а также об отводе земель, недр и акваторий для них;

– дислокации, действительных наименованиях, об организационной структуре, о вооружении, численности войск и состоянии их боевого обеспечения, а также о военно-политической и (или) оперативной обстановке.

2. *Сведения в области экономики, науки и техники*:

– о содержании планов подготовки Российской Федерации к возможным военным действиям, о мобилизационных мощностях промышленности по изготовлению и ремонту вооружения и военной техники, об объемах производства, поставок, о запасах стратегических видов сырья и материалов, а также о размещении, фактических размерах и об использовании государственных материальных резервов;

– об использовании инфраструктуры Российской Федерации в целях обеспечения ее обороноспособности и безопасности;

– о силах и средствах гражданской обороны, дислокации, предназначении и степени защищенности объектов административ-

ного управления, степени обеспечения безопасности населения, о функционировании транспорта и связи в Российской Федерации в целях обеспечения ее безопасности;

– об объемах, о планах (заданиях) государственного оборонного заказа, выпуске и поставках (в денежном или натуральном выражении) вооружения, военной техники и другой оборонной продукции, наличии и наращивании мощностей по их выпуску, о связях предприятий по кооперации, разработчиках или об изготовителях указанных вооружения, военной техники и другой оборонной продукции;

– о достижениях науки и техники, научно-исследовательских, опытно-конструкторских, проектных работах и технологиях, имеющих важное оборонное или экономическое значение и влияющих на безопасность государства;

– о запасах платины, металлов платиновой группы, природных алмазов в Государственном фонде драгоценных металлов и драгоценных камней Российской Федерации, Центральном банке Российской Федерации, а также об объемах запасов в недрах, добычи, производства и потребления стратегических видов полезных ископаемых Российской Федерации (по списку, определяемому Правительством Российской Федерации).

3. *Сведения в области внешней политики и экономики*:

– о внешнеполитической, внешнеэкономической деятельности Российской Федерации, преждевременное распространение которых может нанести ущерб безопасности государства.

– финансовой политике в отношении иностранных государств (за исключением обобщенных показателей по внешней задолженности), а также о финансовой или денежно-кредитной деятельности, преждевременное распространение которых может нанести ущерб безопасности государства.

4. *Сведения в области разведывательной, контрразведывательной и оперативно-розыскной деятельности*:

– о силах, средствах, источниках, методах, планах и результатах разведывательной, контрразведывательной и оперативно-розыскной деятельности, а также данные о финансировании этой деятельности, если эти данные раскрывают перечисленные сведения;

– о лицах, сотрудничающих или сотрудничавших на конфиденциальной основе с органами, осуществляющими разведывательную, контрразведывательную и оперативно-розыскную деятельность;

– об организации, о силах, средствах и методах обеспечения безопасности объектов государственной охраны, а также данные о финансировании этой деятельности, если эти данные раскрывают перечисленные сведения;

– о системе президентской, правительственной, шифрованной, в том числе кодированной и засекреченной связи, о шифрах, раз-

работке, изготовлении шифров и обеспечении ими, о методах и средствах анализа шифровальных средств и средств специальной защиты, об информационно-аналитических системах специального назначения;

– о методах и средствах защиты секретной информации;

– об организации и фактическом состоянии защиты государственной тайны;

– о защите Государственной границы Российской Федерации, исключительной экономической зоны и континентального шельфа Российской Федерации;

– о расходах федерального бюджета, связанных с обеспечением обороны, безопасности государства и правоохранительной деятельности в Российской Федерации;

– о подготовке кадров, мероприятиях, проводимых в целях обеспечения безопасности государства.

Отнесение сведений к государственной тайне осуществляется в соответствии с их отраслевой, ведомственной или программно-целевой принадлежностью, а также в соответствии с законодательством.

Обоснование необходимости отнесения сведений к государственной тайне в соответствии с принципами засекречивания сведений возлагается на органы государственной власти, предприятия, учреждения и организации, которыми эти сведения получены (разработаны).

Отнесение сведений к государственной тайне осуществляется в соответствии с Перечнем сведений, составляющих государственную тайну.

Субъектами отнесения сведений к государственной тайне являются:

1. *Палаты Федерального Собрания*, которые:

– осуществляют законодательное регулирование отношений в области государственной тайны;

– рассматривают статьи федерального бюджета в части средств, направляемых на реализацию государственных программ в области защиты государственной тайны;

– определяют полномочия должностных лиц по обеспечению защиты государственной тайны в аппаратах палат Федерального Собрания.

2. *Президент Российской Федерации*, который:

– утверждает государственные программы в области защиты государственной тайны;

– утверждает по представлению Правительства Российской Федерации состав, структуру межведомственной комиссии по защите государственной тайны и положение о ней;

– утверждает по представлению Правительства Российской Федерации Перечень должностных лиц органов государственной вла-

сти, наделяемых полномочиями по отнесению сведений к государственной тайне, а также Перечень сведений, отнесенных к государственной тайне;

– заключает международные договоры Российской Федерации о совместном использовании и защите сведений, составляющих государственную тайну;

– определяет полномочия должностных лиц по обеспечению защиты государственной тайны в Администрации Президента Российской Федерации;

– в пределах своих полномочий решает иные вопросы, возникающие в связи с отнесением сведений к государственной тайне, их засекречиванием или рассекречиванием и защитой.

3. *Правительство Российской Федерации*, которое:

– организует исполнение Закона Российской Федерации «О государственной тайне»;

– представляет на утверждение Президенту Российской Федерации состав, структуру межведомственной комиссии по защите государственной тайны и положение о ней;

– представляет на утверждение Президенту Российской Федерации Перечень должностных лиц органов государственной власти, наделяемых полномочиями по отнесению сведений к государственной тайне;

– устанавливает порядок разработки Перечня сведений, отнесенных к государственной тайне;

– организует разработку и выполнение государственных программ в области защиты государственной тайны;

– определяет полномочия должностных лиц по обеспечению защиты государственной тайны в аппарате Правительства Российской Федерации;

– устанавливает порядок предоставления социальных гарантий гражданам, допущенным к государственной тайне на постоянной основе, и сотрудникам структурных подразделений по защите государственной тайны;

– устанавливает порядок определения размеров ущерба, наступившего в результате несанкционированного распространения сведений, составляющих государственную тайну, а также ущерба, наносимого собственнику информации в результате ее засекречивания;

– заключает межправительственные соглашения, принимает меры по выполнению международных договоров Российской Федерации о совместном использовании и защите сведений, составляющих государственную тайну, принимает решения о возможности передачи их носителей другим государствам;

– в пределах своих полномочий решает иные вопросы, возникающие в связи с отнесением сведений к государственной тайне, их засекречиванием или рассекречиванием и защитой.

4. *Органы государственной власти Российской Федерации, органы государственной власти субъектов Российской Федерации и органы местного самоуправления* во взаимодействии с органами защиты государственной тайны, расположенными в пределах соответствующих территорий:

– обеспечивают защиту переданных им другими органами государственной власти, предприятиями, учреждениями и организациями сведений, составляющих государственную тайну, а также сведений, засекречиваемых ими;

– обеспечивают защиту государственной тайны на подведомственных им предприятиях, в учреждениях и организациях в соответствии с требованиями актов законодательства Российской Федерации;

– устанавливают размеры предоставляемых социальных гарантий гражданам, допущенным к государственной тайне на постоянной основе, и сотрудникам структурных подразделений по защите государственной тайны на подведомственных им предприятиях, в учреждениях и организациях;

– обеспечивают в пределах своей компетенции проведение проверочных мероприятий в отношении граждан, допускаемых к государственной тайне;

– реализуют предусмотренные законодательством меры по ограничению прав граждан и предоставлению социальных гарантий лицам, имеющим либо имевшим доступ к сведениям, составляющим государственную тайну;

– вносят в полномочные органы государственной власти предложения по совершенствованию системы защиты государственной тайны.

11.3. Порядок засекречивания и рассекречивания

Отнесение сведений к государственной тайне и их засекречивание заключаются во введении в предусмотренном законодательством порядке для сведений, составляющих государственную тайну, ограничений на их распространение и доступ к их носителям.

Отнесение сведений к государственной тайне и их засекречивание осуществляются в соответствии с ***принципами*** законности, обоснованности и своевременности.

Законность отнесения сведений к государственной тайне и их засекречивание заключается в соответствии засекречиваемых сведений законодательству Российской Федерации о государственной тайне.

Обоснованность отнесения сведений к государственной тайне и их засекречивание заключается в установлении путем экспертной оценки целесообразности засекречивания конкретных сведений, вероятных экономических и иных последствий этого акта, исходя

из баланса жизненно важных интересов государства, общества и граждан.

Своевременность отнесения сведений к государственной тайне и их засекречивание заключается в установлении ограничений на распространение их с момента получения (разработки) или заблаговременно.

Не подлежат отнесению к государственной тайне и засекречиванию сведения:

– о чрезвычайных происшествиях и катастрофах, угрожающих безопасности и здоровью граждан и их последствиях, а также о стихийных бедствиях, их официальных прогнозах и последствиях;

– состоянии экологии, здравоохранения, санитарии, демографии, образования, культуры, сельского хозяйства, а также о состоянии преступности;

– привилегиях, компенсациях и социальных гарантиях, предоставляемых государством гражданам, должностным лицам, предприятиям, учреждениям и организациям;

– фактах нарушения прав и свобод человека и гражданина;

– размерах золотого запаса и государственных валютных резервах Российской Федерации;

– состоянии здоровья высших должностных лиц Российской Федерации;

– фактах нарушения законности органами государственной власти и их должностными лицами.

Должностные лица, принявшие решение о засекречивании перечисленных сведений либо о включении их в этих целях в носители сведений, составляющих государственную тайну, несут уголовную, административную или дисциплинарную ответственность в зависимости от причиненного обществу, государству и гражданам материального и морального ущерба. Граждане вправе обжаловать такие решения в суде.

Степень секретности сведений, составляющих государственную тайну, должна соответствовать степени тяжести ущерба, который может быть нанесен безопасности Российской Федерации вследствие распространения указанных сведений.

Устанавливаются три степени секретности сведений, составляющих государственную тайну, и соответствующие этим степеням грифы секретности для носителей указанных сведений: «*Особой важности*», «*Совершенно секретно*» и «*Секретно*».

Порядок определения размеров ущерба, который может быть нанесен безопасности Российской Федерации вследствие распространения сведений, составляющих государственную тайну, и правила отнесения указанных сведений к той или иной степени секретности *устанавливаются Правительством Российской Федерации.*

Использование перечисленных грифов секретности для засекречивания сведений, не отнесенных к государственной тайне, не допускается.

Для осуществления единой государственной политики в области засекречивания сведений ***межведомственная комиссия по защите государственной тайны*** формирует по предложениям органов государственной власти и в соответствии с Перечнем сведений, составляющих государственную тайну, Перечень сведений, отнесенных к государственной тайне. В этом Перечне указываются органы государственной власти, наделяемые полномочиями по распоряжению данными сведениями. Указанный Перечень утверждается Президентом Российской Федерации, подлежит открытому опубликованию и пересматривается по мере необходимости.

Органами государственной власти, руководители которых наделены полномочиями по отнесению сведений к государственной тайне, в соответствии с Перечнем сведений, отнесенных к государственной тайне, разрабатываются развернутые перечни сведений, подлежащих засекречиванию. В эти перечни включаются сведения, полномочиями по распоряжению которыми наделены указанные органы, и устанавливается степень их секретности. В рамках целевых программ по разработке и модернизации образцов вооружения и военной техники, опытно-конструкторских и научно-исследовательских работ по решению заказчиков указанных образцов и работ могут разрабатываться отдельные перечни сведений, подлежащих засекречиванию. Эти перечни утверждаются соответствующими руководителями органов государственной власти. Целесообразность засекречивания таких перечней определяется их содержанием.

Основанием для засекречивания сведений, полученных (разработанных) в результате управленческой, производственной, научной и иных видов деятельности органов государственной власти, предприятий, учреждений и организаций, является их соответствие действующим в данных органах, на данных предприятиях, в данных учреждениях и организациях перечням сведений, подлежащих засекречиванию. При засекречивании этих сведений их носителям присваивается соответствующий гриф секретности.

При невозможности идентификации полученных (разработанных) сведений со сведениями, содержащимися в действующем перечне, должностные лица органов государственной власти, предприятий, учреждений и организаций обязаны обеспечить предварительное засекречивание полученных (разработанных) сведений в соответствии с предполагаемой степенью секретности и в месячный срок направить в адрес должностного лица, утвердившего указанный перечень, предложения по его дополнению (изменению).

Должностные лица, утвердившие действующий перечень, обязаны в течение трех месяцев организовать экспертную оценку поступивших предложений и принять решение по дополнению (изменению) действующего перечня или снятию предварительно присвоенного сведениям грифа секретности.

Рассекречивание сведений и их носителей заключается в снятии ранее введенных в предусмотренном настоящим Законом порядке ограничений на распространение сведений, составляющих государственную тайну, и на доступ к их носителям.

Основаниями для рассекречивания сведений являются: взятие международных обязательств по открытому обмену сведениями, составляющими в Российской Федерации государственную тайну; изменение объективных обстоятельств, вследствие которого дальнейшая защита сведений, составляющих государственную тайну, является нецелесообразной.

Органы государственной власти, руководители которых наделены полномочиями по отнесению сведений к государственной тайне, обязаны периодически, но не реже чем через каждые 5 лет, пересматривать содержание действующих в органах государственной власти, на предприятиях, в учреждениях и организациях перечней сведений, подлежащих засекречиванию, в части обоснованности засекречивания сведений и их соответствия установленной ранее степени секретности.

Срок засекречивания сведений, составляющих государственную тайну, не должен превышать 30 лет. В исключительных случаях этот срок может быть продлен по заключению межведомственной комиссии по защите государственной тайны.

Правом изменения действующих в органах государственной власти, на предприятиях, в учреждениях и организациях *перечней сведений, подлежащих засекречиванию*, наделяются утвердившие их руководители органов государственной власти, которые несут персональную ответственность за обоснованность принятых решений по рассекречиванию сведений. Решения указанных руководителей, связанные с изменением перечня сведений, отнесенных к государственной тайне, подлежат согласованию с межведомственной комиссией по защите государственной тайны, которая вправе приостанавливать и опротестовывать эти решения.

Носители сведений, составляющих государственную тайну, рассекречиваются не позднее сроков, установленных при их засекречивании. До истечения этих сроков носители подлежат рассекречиванию, если изменены положения действующего в данном органе государственной власти, на предприятии, в учреждении и организации перечня, на основании которых они были засекречены.

Руководители органов государственной власти, предприятий, учреждений и организаций наделяются *полномочиями по рассекре-*

чиванию носителей сведений, необоснованно засекреченных подчиненными им должностными лицами.

Граждане, предприятия, учреждения, организации и органы государственной власти Российской Федерации вправе обратиться в органы государственной власти, на предприятия, в учреждения, организации, в том числе в государственные архивы, с запросом о рассекречивании сведений, отнесенных к государственной тайне.

Органы государственной власти, предприятия, учреждения, организации, в том числе государственные архивы, получившие такой запрос, *обязаны* в течение трех месяцев рассмотреть его и дать мотивированный ответ. Если они не правомочны решить вопрос о рассекречивании запрашиваемых сведений, то запрос в месячный срок с момента его поступления передается в орган государственной власти, наделенный такими полномочиями, либо в межведомственную комиссию по защите государственной тайны, о чем уведомляются граждане предприятия, учреждения, организации и органы государственной власти Российской Федерации, подавшие запрос.

Обоснованность отнесения сведений к государственной тайне может быть обжалована в суде. При признании судом необоснованности засекречивания сведений эти сведения подлежат рассекречиванию в установленном законодательством порядке.

11.4. Порядок распоряжения сведениями, составляющими государственную тайну

Взаимная передача сведений, составляющих государственную тайну, осуществляется органами государственной власти, предприятиями, учреждениями и организациями, не состоящими в отношениях подчиненности и не выполняющими совместных работ с санкции органа государственной власти, в распоряжении которого находятся эти сведения.

Органы государственной власти, предприятия, учреждения и организации, запрашивающие сведения, составляющие государственную тайну, обязаны создать условия, обеспечивающие защиту этих сведений. Их руководители несут персональную ответственность за несоблюдение установленных ограничений по ознакомлению со сведениями, составляющими государственную тайну.

Передача сведений, составляющих государственную тайну, предприятиям, учреждениям, организациям или гражданам в связи с выполнением совместных и других работ осуществляется заказчиком этих работ с разрешения органа государственной власти, в распоряжении которого находятся соответствующие сведения, и только в объеме, необходимом для выполнения этих

работ. При этом до передачи сведений заказчик обязан убедиться в наличии у предприятия, учреждения или организации лицензии на проведение работ с использованием сведений соответствующей степени секретности, а у граждан — соответствующего допуска.

Предприятия, учреждения или организации, в том числе и негосударственных форм собственности, при проведении совместных и других работ (получение государственных заказов) и возникновении в связи с этим необходимости в использовании сведений, составляющих государственную тайну, могут заключать с государственными предприятиями, учреждениями или организациями договоры об использовании услуг их структурных подразделений по защите государственной тайны, о чем делается соответствующая отметка обеих договаривающихся сторон в лицензиях на проведение работ с использованием сведений, составляющих государственную тайну.

Организация контроля за эффективностью защиты государственной тайны при проведении совместных и других работ возлагается на заказчика этих работ в соответствии с положениями заключенного сторонами договора.

Решение о передаче сведений, составляющих государственную тайну, другим государствам принимается Правительством Российской Федерации при наличии экспертного заключения межведомственной комиссии по защите государственной тайны о возможности передачи этих сведений.

Обязательства принимающей стороны по защите передаваемых ей сведений предусматриваются заключаемым с ней договором (соглашением).

11.5. Система защиты сведений, составляющих государственную тайну

К *органам защиты государственной тайны* относятся: межведомственная комиссия по защите государственной тайны; федеральные органы исполнительной власти, уполномоченные в области: обеспечения безопасности; обороны; внешней разведки; противодействия техническим разведкам и технической защиты информации и их территориальные органы; органы государственной власти, предприятия, учреждения и организации и их структурные подразделения по защите государственной тайны.

Межведомственная комиссия по защите государственной тайны является коллегиальным органом, координирующим деятельность органов государственной власти по защите государственной тайны в интересах разработки и выполнения государственных программ нормативных и методических документов, обеспечивающих

реализацию законодательства Российской Федерации о государственной тайне.

Функции межведомственной комиссии по защите государственной тайны и ее надведомственные полномочия реализуются в соответствии с Положением о межведомственной комиссии по защите государственной тайны, утверждаемым Президентом Российской Федерации.

Федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности, федеральный орган исполнительной власти, уполномоченный в области обороны, федеральный орган исполнительной власти, уполномоченный в области внешней разведки, федеральный орган исполнительной власти, уполномоченный в области противодействия техническим разведкам и технической защиты информации, и их территориальные органы организуют и обеспечивают защиту государственной тайны в соответствии с функциями, возложенными на них законодательством Российской Федерации.

Органы государственной власти, предприятия, учреждения и организации обеспечивают защиту сведений, составляющих государственную тайну, в соответствии с возложенными на них задачами и в пределах своей компетенции.

Ответственность за организацию защиты сведений, составляющих государственную тайну, в органах государственной власти, на предприятиях в учреждениях и организациях возлагается на их руководителей.

В зависимости от объема работ с использованием сведений, составляющих государственную тайну, руководителями органов государственной власти предприятий, учреждений и организаций создаются структурные подразделения по защите государственной тайны, функции которых определяются указанными руководителями в соответствии с нормативными документами, утверждаемыми Правительством Российской Федерации, и с учетом специфики проводимых ими работ.

Защита государственной тайны является видом основной деятельности органа государственной власти, предприятия, учреждения или организации.

Допуск должностных лиц и граждан Российской Федерации к государственной тайне осуществляется в добровольном порядке.

Допуск к государственной тайне лиц, имеющих двойное гражданство, лиц без гражданства, а также лиц из числа иностранных граждан, эмигрантов и реэмигрантов осуществляется в порядке, устанавливаемом Правительством Российской Федерации.

Допуск должностных лиц и граждан к государственной тайне предусматривает:

– принятие на себя обязательств перед государством по нераспространению доверенных им сведений, составляющих государственную тайну;

– согласия на частичные, временные ограничения их прав в соответствии с законодательством;

– письменное согласие на проведение проверочных мероприятий полномочными органами;

– определение видов, размеров и порядка предоставления социальных гарантий, предусмотренных законодательством;

– ознакомление с нормами законодательства Российской Федерации о государственной тайне, предусматривающими ответственность за его нарушение;

– принятие решения руководителем органа государственной власти, предприятия, учреждения или организации об оформлении допуска лица к сведениям, составляющим государственную тайну.

Объем проверочных мероприятий зависит от степени секретности сведений. Проверочные мероприятия осуществляются в соответствии с законодательством Российской Федерации.

Для должностных лиц и граждан, допущенных к государственной тайне на постоянной основе, устанавливаются следующие *социальные гарантии*: процентные надбавки к заработной плате в зависимости от степени секретности сведений, к которым они имеют доступ; преимущественное право при прочих равных условиях на оставление на работе при проведении органами государственной власти, предприятиями, учреждениями и организациями организационных и (или) штатных мероприятий.

Для сотрудников структурных подразделений по защите государственной тайны дополнительно к социальным гарантиям устанавливается процентная надбавка к заработной плате за стаж работы в указанных структурных подразделениях.

Установлены ***три формы допуска к государственной тайне должностных лиц и граждан***, соответствующие трем степеням секретности сведений, составляющих государственную тайну: *к сведениям особой важности, совершенно секретным или секретным*. Наличие у должностных лиц и граждан допуска к сведениям более высокой степени секретности является основанием для доступа их к сведениям более низкой степени секретности.

Сроки, обстоятельства и порядок переоформления допуска граждан к государственной тайне устанавливаются нормативными документами, утверждаемыми Правительством Российской Федерации.

Порядок допуска должностных лиц и граждан к государственной тайне в условиях объявленного чрезвычайного положения может быть изменен Президентом Российской Федерации.

Члены Совета Федерации, депутаты Государственной Думы, судьи на период исполнения ими своих полномочий, а также адвокаты, участвующие в качестве защитников в уголовном судопроизводстве по делам, связанным со сведениями, составляющи-

ми государственную тайну, допускаются к этим сведениям без проведения проверочных мероприятий. Указанные лица предупреждаются о неразглашении государственной тайны, ставшей известной в связи с исполнением ими своих полномочий, и о привлечении их к ответственности в случае ее разглашения, о чем у них берется соответствующая расписка.

Сохранность государственной тайны в таких случаях гарантируется путем установления ответственности указанных лиц федеральным законом.

Основаниями для отказа должностному лицу или гражданину в допуске к государственной тайне может быть:

– признание его судом недееспособным, ограниченно дееспособным или рецидивистом, нахождение его под судом или следствием за государственные и иные тяжкие преступления, наличие неснятой судимости за эти преступления;

– наличие медицинских противопоказаний для работы с использованием сведений, составляющих государственную тайну, согласно перечню, утверждаемому федеральным органом исполнительной власти, уполномоченным в области здравоохранения и социального развития;

– постоянное проживание его самого и (или) его близких родственников за границей и (или) оформление указанными лицами документов для выезда на постоянное жительство в другие государства;

– выявление в результате проверочных мероприятий оформляемого лица действий, создающих угрозу безопасности Российской Федерации;

– уклонение его от проверочных мероприятий и (или) сообщение им заведомо ложных анкетных данных.

Решение об отказе должностному лицу или гражданину в допуске к государственной тайне принимается руководителем органа государственной власти, предприятия, учреждения или организации в индивидуальном порядке с учетом результатов проверочных мероприятий. Гражданин имеет право обжаловать это решение в вышестоящей организации или в суде.

Допуск должностного лица или гражданина к государственной тайне может быть прекращен по решению руководителя органа государственной власти, предприятия, учреждения или организации в случаях:

– расторжения с ним трудового договора (контракта) в связи с проведением организационных и (или) штатных мероприятий;

– однократного нарушения им взятых обязательств, предусмотренных трудовым договором (контрактом);

– возникновения обстоятельств, являющихся основанием для отказа должностному лицу или гражданину в допуске к государственной тайне.

Прекращение допуска должностного лица или гражданина к государственной тайне:

– является дополнительным основанием для расторжения с ним трудового договора (контракта), если такие условия предусмотрены в трудовом договоре (контракте);

– не освобождает должностное лицо или гражданина от взятых ими обязательств по неразглашению сведений, составляющих государственную тайну.

Решение администрации о прекращении допуска должностного лица или гражданина к государственной тайне и расторжении на основании этого трудового договора (контракта) может быть обжаловано в вышестоящей организации или в суде.

Должностное лицо или гражданин, допущенные или ранее допускавшиеся к государственной тайне, могут быть временно ограничены в своих правах. Ограничения могут касаться:

– права выезда за границу на срок, оговоренный в трудовом договоре (контракте) при оформлении допуска гражданина к государственной тайне;

– права на распространение сведений, составляющих государственную тайну, и на использование открытий и изобретений, содержащих такие сведения;

– права на неприкосновенность частной жизни при проведении проверочных мероприятий в период оформления допуска к государственной тайне.

Организация доступа должностного лица или гражданина к сведениям, составляющим государственную тайну, возлагается на руководителя соответствующего органа государственной власти, предприятия, учреждения или организации, а также на их структурные подразделения по защите государственной тайны. Порядок доступа должностного лица или гражданина к сведениям, составляющим государственную тайну, устанавливается нормативными документами, утверждаемыми Правительством Российской Федерации.

Руководители органов государственной власти, предприятий, учреждений и организаций несут персональную ответственность за создание таких условий, при которых должностное лицо или гражданин знакомятся только с теми сведениями, составляющими государственную тайну, и в таких объемах, которые необходимы ему для выполнения должностных (функциональных) обязанностей.

Контрольные вопросы

1. В чем заключается предмет и цель правового регулирования отношений в области государственной тайны?

2. Раскройте структуру правового режима государственной тайны.

3. Перечислите виды сведений, которые составляют государственную тайну.

4. В чем заключается порядок отнесения сведений к государственной тайне?

5. Каков порядок рассекречивания сведений, составляющих государственную тайну?

6. Каков порядок распоряжения сведениями, составляющими государственную тайну?

7. Раскройте структуру системы сведений, составляющих государственную тайну.

Глава 12

ЗАКОНОДАТЕЛЬСТВО ОБ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ

12.1. Общие положения

Законодательство в области электронной цифровой подписи составляет Гражданский кодекс Российской Федерации, Федеральный закон «Об электронной цифровой подписи», Федеральный закон «Об информации, информационных технологиях и о защите информации», Федеральный закон «О связи», другие федеральные законы и принимаемые в соответствии с ними иные нормативные правовые акты Российской Федерации.

Предмет правового регулирования в области электронной цифровой подписи составляет совокупность отношений, возникающих при совершении гражданско-правовых сделок с использованием электронных документов и в других предусмотренных законодательством Российской Федерации случаях.

Цель правового регулирования заключается в обеспечении правовых условий использования электронной цифровой подписи в электронных документах, при соблюдении которых подпись в документе признается равнозначной собственноручной подписи в документе на бумажном носителе.

При правовом регулировании используются следующие понятия:

– *электронный документ* — документ, в котором информация представлена в электронно-цифровой форме;

– *электронная цифровая подпись* — реквизит электронного документа, предназначенный для его защиты от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе;

– *средства электронной цифровой подписи* — аппаратные и (или) программные средства, обеспечивающие реализацию хотя бы одной из следующих функций: создание электронной цифровой подписи в электронном документе с использованием закрытого ключа электронной цифровой подписи; подтверждение с использованием открытого ключа электронной цифровой подписи ее подлинности электронной цифровой подписи в электронном документе; создание закрытых и открытых ключей электронных цифровых подписей;

– *закрытый ключ электронной цифровой подписи* — уникальная последовательность символов, известная владельцу сертификата ключа подписи и предназначенная для создания в электронных документах электронной цифровой подписи с использованием средств электронной цифровой подписи;

– *открытый ключ электронной цифровой подписи* — уникальная последовательность символов, соответствующая закрытому ключу электронной цифровой подписи, доступная любому пользователю информационной системы и предназначенная для подтверждения подлинности электронной цифровой подписи в электронном документе;

– *сертификат ключа подписи* — документ на бумажном носителе или электронный документ с электронной цифровой подписью уполномоченного лица удостоверяющего центра, которые включают открытый ключ электронной цифровой подписи и выдаются удостоверяющим центром участнику информационной системы для подтверждения подлинности электронной цифровой подписи и идентификации владельца сертификата ключа подписи;

– *владелец сертификата ключа подписи* — физическое лицо, на имя которого удостоверяющим центром выдан сертификат ключа подписи и которое владеет соответствующим закрытым ключом электронной цифровой подписи, позволяющим с помощью средств электронной цифровой подписи создавать свою электронную цифровую подпись в электронных документах (подписывать электронные документы);

– *пользователь сертификата ключа подписи* — физическое лицо, использующее полученные в удостоверяющем центре сведения о сертификате ключа подписи для проверки принадлежности электронной цифровой подписи владельцу сертификата ключа подписи;

– *сертификат средств электронной цифровой подписи* — документ на бумажном носителе, выданный в соответствии с правилами системы сертификации для подтверждения соответствия средств электронной цифровой подписи установленным требованиям;

– *подтверждение подлинности электронной цифровой подписи в электронном документе* — положительный результат проверки соответствующим сертифицированным средством электронной цифровой подписи с использованием сертификата ключа подписи принадлежности электронной цифровой подписи в электронном документе владельцу сертификата ключа подписи и отсутствие искажений в подписанном данной электронной цифровой подписью электронном документе;

– *информационная система общего пользования* — информационная система, которая открыта для использования всеми физическими и юридическими лицами и в услугах которой этим лицам не может быть отказано;

– *корпоративная информационная система* — информационная система, участниками которой может быть ограниченный круг лиц, определенный ее владельцем или соглашением участников этой информационной системы.

В основу правового регулирования отношений в рассматриваемой области положен ***режим электронной цифровой подписи***, включающий: условия признания равнозначности электронной цифрой подписи и собственноручной подписи; институты сертификата ключа электронной цифровой подписи и владельца сертификата; институт удостоверяющих центров.

12.2. Условия признания равнозначности электронной цифровой подписи и собственноручной подписи

Электронная цифровая подпись в электронном документе равнозначна собственноручной подписи в документе на бумажном носителе при одновременном соблюдении следующих условий:

– сертификат ключа подписи, относящийся к этой электронной цифровой подписи, не утратил силу (действует) на момент проверки или на момент подписания электронного документа при наличии доказательств, определяющих момент подписания;

– подтверждена подлинность электронной цифровой подписи в электронном документе;

– электронная цифровая подпись используется в соответствии со сведениями, указанными в сертификате ключа подписи.

Участник информационной системы может быть одновременно владельцем любого количества сертификатов ключей подписей. При этом электронный документ с электронной цифровой подписью имеет юридическое значение при осуществлении отношений, указанных в сертификате ключа подписи.

Создание ключей электронных цифровых подписей осуществляется для использования в информационной системе общего пользования ее участником или по его обращению удостоверяющим центром, корпоративной информационной системе в порядке, установленном в этой системе.

При создании ключей электронных цифровых подписей для использования в информационной системе общего пользования должны применяться только сертифицированные средства электронной цифровой подписи. Возмещение убытков, причиненных в связи с созданием ключей электронных цифровых подписей несертифицированными средствами электронной цифровой подписи, может быть возложено на создателей и распространителей этих средств в соответствии с законодательством Российской Федерации.

Использование несертифицированных средств электронной цифровой подписи и созданных ими ключей электронных цифровых подписей в корпоративных информационных системах феде-

ральных органов государственной власти, органов государственной власти субъектов Российской Федерации и органов местного самоуправления не допускается.

Сертификация средств электронной цифровой подписи осуществляется в соответствии с законодательством Российской Федерации о сертификации продукции и услуг.

12.3. Институты сертификата ключа электронной цифровой подписи и владельца сертификата

Сертификат ключа подписи должен содержать:

– уникальный регистрационный номер сертификата ключа подписи, дату начала и окончания срока действия сертификата ключа подписи, находящегося в реестре удостоверяющего центра;

– фамилию, имя и отчество владельца сертификата ключа подписи или псевдоним владельца. В случае использования псевдонима удостоверяющим центром вносится запись об этом в сертификат ключа подписи;

– открытый ключ электронной цифровой подписи;

– наименование средств электронной цифровой подписи, с которыми используется данный открытый ключ электронной цифровой подписи;

– наименование и место нахождения удостоверяющего центра, выдавшего сертификат ключа подписи;

– сведения об отношениях, при осуществлении которых электронный документ с электронной цифровой подписью будет иметь юридическое значение.

В случае необходимости в *сертификате ключа подписи на основании подтверждающих документов указываются должность* (с указанием наименования и места нахождения организации, в которой установлена эта должность) и *квалификация владельца сертификата ключа подписи*, а по его заявлению в письменной форме — иные сведения, подтверждаемые соответствующими документами.

Сертификат ключа подписи должен быть внесен удостоверяющим центром в реестр сертификатов ключей подписей не позднее даты начала действия сертификата.

Для проверки принадлежности электронной цифровой подписи соответствующему владельцу сертификат ключа подписи выдается пользователям с указанием даты и времени его выдачи, сведений о действии сертификата (действует, действие приостановлено, сроки приостановления его действия, аннулирован, дата и время аннулирования) и сведений о реестре сертификатов ключей подписей. В случае выдачи сертификата ключа подписи в форме документа на бумажном носителе он оформляется на бланке удостоверяющего центра и заверяется собственноручной подпи-

сью уполномоченного лица и печатью удостоверяющего центра. В случае выдачи сертификата ключа подписи и указанных дополнительных данных в форме электронного документа этот сертификат должен быть подписан электронной цифровой подписью уполномоченного лица удостоверяющего центра.

Владелец сертификата ключа подписи обязан:

– не использовать для электронной цифровой подписи открытые и закрытые ключи электронной цифровой подписи, если ему известно, что эти ключи используются или использовались ранее;

– хранить в тайне закрытый ключ электронной цифровой подписи;

– немедленно требовать приостановления действия сертификата ключа подписи при наличии оснований полагать, что тайна закрытого ключа подписи нарушена.

При несоблюдении данных условий возмещение причиненных убытков возлагается на владельца сертификата ключа подписи.

12.4. Институт удостоверяющих центров

Удостоверяющим центром, выдающим сертификаты ключей подписей для использования в информационных системах общего пользования, должно быть юридическое лицо, выполняющее функции, предусмотренные законодательством. При этом удостоверяющий центр должен обладать необходимыми материальными и финансовыми возможностями, позволяющими ему нести гражданскую ответственность перед пользователями сертификатов ключей подписей за убытки, которые могут быть понесены ими вследствие недостоверности сведений, содержащихся в сертификатах ключей подписей.

Требования, предъявляемые к материальным и финансовым возможностям удостоверяющих центров, определяются Правительством Российской Федерации по представлению уполномоченного федерального органа исполнительной власти.

Статус удостоверяющего центра, обеспечивающего функционирование корпоративной информационной системы, определяется ее владельцем или соглашением участников этой системы.

Деятельность удостоверяющего центра подлежит лицензированию в соответствии с законодательством Российской Федерации о лицензировании отдельных видов деятельности.

Удостоверяющий центр выполняет следующие функции:

– изготавливает сертификаты ключей подписей;

– создает ключи электронных цифровых подписей по обращению участников информационной системы с гарантией сохранения в тайне закрытого ключа электронной цифровой подписи;

– приостанавливает и возобновляет действие сертификатов ключей подписей, а также аннулирует их;

– ведет реестр сертификатов ключей подписей, обеспечивает его актуальность и возможность свободного доступа к нему участников информационных систем;

– проверяет уникальность открытых ключей электронных цифровых подписей в реестре сертификатов ключей подписей и архиве удостоверяющего центра;

– выдает сертификаты ключей подписей в форме документов на бумажных носителях и (или) в форме электронных документов с информацией об их действии;

– осуществляет по обращениям пользователей сертификатов ключей подписей подтверждение подлинности электронной цифровой подписи в электронном документе в отношении выданных им сертификатов ключей подписей;

– может предоставлять участникам информационных систем иные услуги, связанные с использованием электронных цифровых подписей.

Изготовление сертификатов ключей подписей осуществляется на основании заявления участника информационной системы, которое содержит сведения, указанные в законодательстве и необходимые для идентификации владельца сертификата ключа подписи и передачи ему сообщений. Заявление подписывается собственноручно владельцем сертификата ключа подписи. Содержащиеся в заявлении сведения подтверждаются предъявлением соответствующих документов.

При изготовлении сертификатов ключей подписей удостоверяющим центром оформляются в форме документов на бумажных носителях два экземпляра сертификата, которые заверяются собственноручными подписями владельца сертификата и уполномоченного лица удостоверяющего центра, а также печатью удостоверяющего центра. Один экземпляр сертификата ключа подписи выдается владельцу сертификата ключа подписи, второй — остается в удостоверяющем центре.

Услуги по выдаче участникам информационных систем сертификатов ключей подписей, зарегистрированных удостоверяющим центром, одновременно с информацией об их действии в форме электронных документов оказываются безвозмездно.

Удостоверяющий центр до начала использования электронной цифровой подписи уполномоченного лица удостоверяющего центра для заверения от имени удостоверяющего центра сертификатов ключей подписей обязан представить в уполномоченный федеральный орган исполнительной власти сертификат ключа подписи уполномоченного лица удостоверяющего центра в форме электронного документа, а также этот сертификат в форме документа на бумажном носителе с собственноручной подписью указанного уполномоченного лица, заверенный подписью руководителя и печатью удостоверяющего центра.

Уполномоченный федеральный орган исполнительной власти ведет единый государственный реестр сертификатов ключей подписей (удостоверяющие центры, работающие с участниками информационных систем общего пользования, заверяют выдаваемые ими сертификаты ключей подписей), обеспечивает возможность свободного доступа к этому реестру и выдает сертификаты ключей подписей соответствующих уполномоченных лиц удостоверяющих центров.

Электронные цифровые подписи уполномоченных лиц удостоверяющих центров могут использоваться только после включения их в единый государственный реестр сертификатов ключей подписей. Использование этих электронных цифровых подписей для целей, не связанных с заверением сертификатов ключей подписей и сведений об их действии, не допускается.

Уполномоченный федеральный орган исполнительной власти осуществляет:

– по обращениям физических лиц, организаций, федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации и органов местного самоуправления подтверждение подлинности электронных цифровых подписей уполномоченных лиц удостоверяющих центров в выданных ими сертификатах ключей подписей;

– в соответствии с положением об уполномоченном федеральном органе исполнительной власти иные полномочия по обеспечению действия Федерального закона «Об электронной цифровой подписи».

Удостоверяющий центр при изготовлении сертификата ключа подписи принимает следующие обязательства по отношению к владельцу сертификата ключа подписи:

– вносить сертификат ключа подписи в реестр сертификатов ключей подписей;

– обеспечивать выдачу сертификата ключа подписи обратившимся к нему участникам информационных систем;

– приостанавливать действие сертификата ключа подписи по обращению его владельца;

– уведомлять владельца сертификата ключа подписи о фактах, которые стали известны удостоверяющему центру и которые существенным образом могут сказаться на возможности дальнейшего использования сертификата ключа подписи;

– иные установленные нормативными правовыми актами или соглашением сторон обязательства.

Срок хранения сертификата ключа подписи в форме электронного документа в удостоверяющем центре *определяется договором* между удостоверяющим центром и владельцем сертификата ключа подписи. При этом обеспечивается доступ участников информационной системы в удостоверяющий центр для получения сертификата ключа подписи.

Срок хранения сертификата ключа подписи в форме электронного документа в удостоверяющем центре после аннулирования сертификата ключа подписи должен быть не менее установленного законодательством срока исковой давности для отношений, указанных в сертификате ключа подписи.

По истечении указанного срока хранения сертификат ключа подписи исключается из реестра и переводится в режим архивного хранения. Срок архивного хранения составляет не менее пяти лет. Порядок выдачи копий сертификатов ключей подписей в этот период устанавливается в соответствии с законодательством Российской Федерации.

Сертификат ключа подписи в форме документа на бумажном носителе хранится в порядке, установленном законодательством Российской Федерации об архивах и архивном деле.

Действие сертификата ключа подписи может быть приостановлено удостоверяющим центром на основании указания лиц или органов, имеющих такое право в силу закона или договора, а в корпоративной информационной системе также в силу установленных для нее правил пользования.

Период от поступления в удостоверяющий центр указания о приостановлении действия сертификата ключа подписи до внесения соответствующей информации в реестр сертификатов ключей подписей должен устанавливаться в соответствии с общим для всех владельцев сертификатов ключей подписей правилом. По договоренности между удостоверяющим центром и владельцем сертификата ключа подписи этот период может быть сокращен.

Действие сертификата ключа подписи по указанию полномочного лица (органа) приостанавливается на исчисляемый в днях срок, если иное не установлено нормативными правовыми актами или договором. Удостоверяющий центр возобновляет действие сертификата ключа подписи по указанию полномочного лица (органа). В случае, если по истечении указанного срока не поступает указание о возобновлении действия сертификата ключа подписи, он подлежит аннулированию.

В соответствии с указанием полномочного лица (органа) о приостановлении действия сертификата ключа подписи удостоверяющий центр оповещает об этом пользователей сертификатов ключей подписей путем внесения в реестр сертификатов ключей подписей соответствующей информации с указанием даты, времени и срока приостановления действия сертификата ключа подписи, а также извещает об этом владельца сертификата ключа подписи и полномочное лицо (орган), от которого получено указание о приостановлении действия сертификата ключа подписи.

Удостоверяющий центр, выдавший сертификат ключа подписи, обязан аннулировать его:

– по истечении срока действия;

– при утрате юридической силы сертификата соответствующих средств электронной цифровой подписи, используемых в информационных системах общего пользования;

– в случае, если удостоверяющему центру стало достоверно известно о прекращении действия документа, на основании которого оформлен сертификат ключа подписи;

– по заявлению в письменной форме владельца сертификата ключа подписи;

– в иных установленных нормативными правовыми актами или соглашением сторон случаях.

В случае аннулирования сертификата ключа подписи удостоверяющий центр оповещает об этом пользователей сертификатов ключей подписей путем внесения в реестр сертификатов ключей подписей соответствующей информации с указанием даты и времени аннулирования сертификата ключа подписи, за исключением случаев аннулирования сертификата по истечении срока его действия, а также извещает об этом владельца сертификата ключа подписи и полномочное лицо (орган), от которого получено указание об аннулировании сертификата.

Деятельность удостоверяющего центра, выдающего сертификаты ключей подписей для использования в информационных системах общего пользования, *может быть прекращена* в порядке, установленном гражданским законодательством.

В случае прекращения деятельности удостоверяющего центра сертификаты ключей подписей, выданные этим удостоверяющим центром, могут быть переданы другому удостоверяющему центру по согласованию с владельцами сертификатов ключей подписей.

Сертификаты ключей подписей, не переданные в другой удостоверяющий центр, аннулируются и передаются на хранение уполномоченному федеральному органу исполнительной власти.

Деятельность удостоверяющего центра, обеспечивающего функционирование корпоративной информационной системы, прекращается по решению владельца этой системы, а также по договоренности участников этой системы в связи с передачей обязательств данного удостоверяющего центра другому удостоверяющему центру или в связи с ликвидацией корпоративной информационной системы.

12.5. Особенности использования электронной цифровой подписи

Федеральные органы государственной власти, органы государственной власти субъектов Российской Федерации, органы местного самоуправления, а также организации, участвующие в документообороте с указанными органами, используют для подписания своих электронных документов электронные цифровые подписи уполномоченных лиц указанных органов и организаций.

Сертификаты ключей подписей уполномоченных лиц федеральных органов государственной власти включаются в реестр сертификатов ключей подписей, который ведется уполномоченным федеральным органом исполнительной власти, и выдаются пользователям сертификатов ключей подписей из этого реестра в порядке, установленном законодательством для удостоверяющих центров.

Порядок организации выдачи сертификатов ключей подписей уполномоченных лиц органов государственной власти субъектов Российской Федерации и уполномоченных лиц органов местного самоуправления устанавливается нормативными правовыми актами соответствующих органов.

Корпоративная информационная система, предоставляющая участникам информационной системы общего пользования услуги удостоверяющего центра корпоративной информационной системы, должна соответствовать требованиям, установленным для информационных систем общего пользования.

Порядок использования электронных цифровых подписей в корпоративной информационной системе устанавливается решением владельца корпоративной информационной системы или соглашением участников этой системы.

Содержание информации в сертификатах ключей подписей, порядок ведения реестра сертификатов ключей подписей, порядок хранения аннулированных сертификатов ключей подписей, случаи утраты указанными сертификатами юридической силы в корпоративной информационной системе регламентируются решением владельца этой системы или соглашением участников корпоративной информационной системы.

Иностранный сертификат ключа подписи, удостоверенный в соответствии с законодательством иностранного государства, в котором этот сертификат ключа подписи зарегистрирован, признается на территории Российской Федерации в случае выполнения установленных законодательством Российской Федерации процедур признания юридического значения иностранных документов.

Содержание документа на бумажном носителе, заверенного печатью и преобразованного в электронный документ, в соответствии с нормативными правовыми актами или соглашением сторон может заверяться электронной цифровой подписью уполномоченного лица.

В случаях, установленных законами и иными нормативными правовыми актами Российской Федерации или соглашением сторон, *электронная цифровая подпись в электронном документе, сертификат которой содержит необходимые при осуществлении данных отношений сведения о правомочиях его владельца, признается равнозначной собственноручной подписи* лица в документе на бумажном носителе, заверенном печатью.

Контрольные вопросы

1. Раскройте содержание правового режима электронной цифровой подписи.
2. Что такое «сертификат ключа электронной цифровой подписи» и зачем он нужен?
3. Раскройте содержание правового статуса удостоверяющего центра.

Глава 13

ЗАКОНОДАТЕЛЬСТВО О ТЕХНИЧЕСКОМ РЕГУЛИРОВАНИИ

13.1. Общие положения

Законодательство Российской Федерации о техническом регулировании состоит из Федерального закона «О техническом регулировании», принимаемых в соответствии с ним федеральных законов и иных нормативных правовых актов Российской Федерации.

Предметом правового регулирования в рассматриваемой области являются отношения, возникающие при: разработке, принятии, применении и исполнении обязательных требований к продукции, процессам производства, эксплуатации, хранения, перевозки, реализации и утилизации; разработке, принятии, применении и исполнении на добровольной основе требований к продукции, процессам производства, эксплуатации, хранения, перевозки, реализации и утилизации, выполнению работ или оказанию услуг; оценке соответствия.

Основными источниками технических требований, устанавливаемых в рамках технического регулирования, являются: технические регламенты; стандарты.

13.2. Технические регламенты

Под техническим регламентом понимается документ, который принят международным договором Российской Федерации, ратифицированным в порядке, установленном законодательством Российской Федерации, федеральным законом или указом Президента Российской Федерации, или постановлением Правительства Российской Федерации, и устанавливает обязательные для применения и исполнения требования к объектам технического регулирования (продукции, в том числе зданиям, строениям и сооружениям, процессам производства, эксплуатации, хранения, перевозки, реализации и утилизации).

Технические регламенты принимаются в следующих целях:

– защита жизни или здоровья граждан, имущества физических или юридических лиц, государственного или муниципального имущества;

– охрана окружающей среды, жизни или здоровья животных и растений;

– предупреждение действий, вводящих в заблуждение приобретателей.

Принятие технических регламентов в иных целях не допускается.

Технические регламенты с учетом степени риска причинения вреда *устанавливают минимально необходимые требования, обеспечивающие* безопасность излучений; биологическую безопасность; взрывобезопасность; механическую безопасность; пожарную безопасность; промышленную безопасность; термическую безопасность; химическую безопасность; электрическую безопасность; ядерную и радиационную безопасность; электромагнитную совместимость в части обеспечения безопасности работы приборов и оборудования; единство измерений.

Технический регламент должен содержать исчерпывающий перечень продукции, процессов производства, эксплуатации, хранения, перевозки, реализации и утилизации, в отношении которых устанавливаются его требования, и правила идентификации объекта технического регулирования для целей применения технического регламента, требования к характеристикам продукции, процессам производства, эксплуатации, хранения, перевозки, реализации и утилизации, но не должен содержать требования к конструкции и исполнению, за исключением случаев, если из-за отсутствия требований к конструкции и исполнению с учетом степени риска причинения вреда не обеспечивается достижение целей принятия технического регламента.

В *технических регламентах* с учетом степени риска причинения вреда *могут содержаться специальные требования* к продукции, процессам производства, эксплуатации, хранения, перевозки, реализации и утилизации, требования к терминологии, упаковке, маркировке или этикеткам и правилам их нанесения, обеспечивающие защиту отдельных категорий граждан (несовершеннолетних, беременных женщин, кормящих матерей, инвалидов).

Оценка соответствия проводится в формах государственного контроля (надзора), аккредитации, испытания, регистрации, подтверждения соответствия, приемки и ввода в эксплуатацию объекта, строительство которого закончено, и в иной форме.

Правила и методы исследований (испытаний) и измерений, а также правила отбора образцов для проведения исследований (испытаний) и измерений, необходимые для применения технических регламентов, разрабатываются с соблюдением положений законодательства федеральными органами исполнительной власти в пределах их компетенции в течение шести месяцев со дня официального опубликования технических регламентов и утверждаются Правительством Российской Федерации.

Выделяют следующие *виды технических регламентов*: общие технические регламенты; специальные технические регламенты.

Требования *общего технического регламента* обязательны для применения и соблюдения в отношении любых видов продукции, процессов производства, эксплуатации, хранения, перевозки, реализации и утилизации. *Эти регламенты принимаются по следующим вопросам*:

– безопасная эксплуатация и утилизация машин и оборудования;

– безопасная эксплуатация зданий, строений, сооружений и безопасное использование прилегающих к ним территорий;

– пожарная безопасность;

– биологическая безопасность;

– электромагнитная совместимость;

– экологическая безопасность;

– ядерная и радиационная безопасность.

Требованиями *специального технического регламента* учитываются технологические и иные особенности отдельных видов продукции, процессов производства, эксплуатации, хранения, перевозки, реализации и утилизации и устанавливаются требования только к тем отдельным видам продукции, процессам производства, эксплуатации, хранения, перевозки, реализации и утилизации, степень риска причинения вреда которыми выше степени риска причинения вреда, учтенной общим техническим регламентом.

Технический регламент принимается федеральным законом.

В случае отсутствия требований технических регламентов в отношении оборонной продукции (работ, услуг), поставляемой для федеральных государственных нужд по государственному оборонному заказу, продукции (работ, услуг), используемой в целях защиты сведений, составляющих государственную тайну или относимых к охраняемой в соответствии с законодательством Российской Федерации информации ограниченного доступа, продукции (работ, услуг), сведения о которой составляют государственную тайну, обязательными являются требования к продукции, ее характеристикам и требования к процессам производства, эксплуатации, хранения, перевозки, реализации и утилизации, установленные федеральными органами исполнительной власти, являющимися в пределах своей компетенции государственными заказчиками оборонного заказа, и (или) государственным контрактом.

13.3. Стандарты

Под стандартом понимается документ, в котором в целях добровольного многократного использования устанавливаются характеристики продукции, правила осуществления и характеристики процессов производства, эксплуатации, хранения, перевозки, реализации и утилизации, выполнения работ или оказания услуг.

Стандарт также может содержать требования к терминологии, символике, упаковке, маркировке или этикеткам и правилам их нанесения. Деятельность по установлению правил и характеристик в целях их добровольного многократного использования, направленная на достижение упорядоченности в сферах производства и обращения продукции и повышение конкурентоспособности продукции, работ или услуг, называется *стандартизацией.*

Стандартизация осуществляется в следующих целях:

– повышение уровня безопасности жизни или здоровья граждан, имущества физических или юридических лиц, государственного или муниципального имущества, экологической безопасности, безопасности жизни или здоровья животных и растений, содействие соблюдению требований технических регламентов;

– повышение уровня безопасности объектов с учетом риска возникновения чрезвычайных ситуаций природного и техногенного характера;

– обеспечение научно-технического прогресса;

– повышение конкурентоспособности продукции, работ, услуг;

– рациональное использование ресурсов;

– техническая и информационная совместимость;

– сопоставимость результатов исследований (испытаний) и измерений, технических и экономико-статистических данных;

– взаимозаменяемость продукции.

Стандартизация осуществляется в соответствии со следующими принципами:

– добровольного применения стандартов;

– максимального учета при разработке стандартов законных интересов заинтересованных лиц;

– применения международного стандарта как основы разработки национального стандарта, за исключением случаев, если такое применение признано невозможным вследствие несоответствия требований международных стандартов климатическим и географическим особенностям Российской Федерации, техническим и (или) технологическим особенностям или по иным основаниям либо Российская Федерация в соответствии с установленными процедурами выступала против принятия международного стандарта или отдельного его положения;

– недопустимости создания препятствий производству и обращению продукции, выполнению работ и оказанию услуг в большей степени, чем это минимально необходимо для выполнения целей стандартизации;

– недопустимости установления таких стандартов, которые противоречат техническим регламентам;

– обеспечения условий для единообразного применения стандартов.

К *документам в области стандартизации*, используемым на территории Российской Федерации, относятся: национальные стандарты; правила стандартизации, нормы и рекомендации в области стандартизации; применяемые в установленном порядке классификации, общероссийские классификаторы технико-экономической и социальной информации; стандарты организаций.

Национальные стандарты и общероссийские классификаторы технико-экономической и социальной информации, в том числе правила их разработки и применения, представляют собой *национальную систему стандартизации*.

Национальный стандарт применяется на добровольной основе равным образом и в равной мере независимо от страны и (или) места происхождения продукции, осуществления процессов производства, эксплуатации, хранения, перевозки, реализации и утилизации, выполнения работ и оказания услуг, видов или особенностей сделок и (или) лиц, являющихся изготовителями, исполнителями, продавцами, приобретателями.

Применение национального стандарта подтверждается знаком соответствия национальному стандарту. Разработчиком национального стандарта может быть любое лицо.

Общероссийские классификаторы технико-экономической и социальной информации (далее — общероссийские классификаторы) — это нормативные документы, распределяющие технико-экономическую и социальную информацию в соответствии с ее классификацией (классами, группами, видами и другим) и являющиеся обязательными для применения при создании государственных информационных систем и информационных ресурсов и межведомственном обмене информацией.

Порядок разработки, принятия, введения в действие, ведения и применения общероссийских классификаторов в социально-экономической области (в том числе в области прогнозирования, статистического учета, банковской деятельности, налогообложения, при межведомственном информационном обмене, создании информационных систем и информационных ресурсов) устанавливается Правительством Российской Федерации.

Стандарты организаций, в том числе коммерческих, общественных, научных, саморегулируемых, объединений юридических лиц, могут разрабатываться и утверждаться ими самостоятельно, исходя из необходимости применения их для целей стандартизации, для совершенствования производства и обеспечения качества продукции, выполнения работ, оказания услуг, а также для распространения и использования полученных в различных областях знаний результатов исследований (испытаний), измерений и разработок.

Стандарты организаций применяются равным образом и в равной мере независимо от страны и (или) места происхождения продукции, осуществления процессов производства, эксплуата-

ции, хранения, перевозки, реализации и утилизации, выполнения работ и оказания услуг, видов или особенностей сделок и (или) лиц, которые являются изготовителями, исполнителями, продавцами, приобретателями.

13.4. Подтверждение соответствия техническим регламентам и стандартам

Под подтверждением соответствия понимается документальное удостоверение соответствия продукции или иных объектов, процессов производства, эксплуатации, хранения, перевозки, реализации и утилизации, выполнения работ или оказания услуг требованиям технических регламентов, положениям стандартов или условиям договоров.

Подтверждение соответствия осуществляется в следующих целях:

– удостоверение соответствия продукции, процессов производства, эксплуатации, хранения, перевозки, реализации и утилизации, работ, услуг или иных объектов техническим регламентам, стандартам, условиям договоров;

– содействие приобретателям в компетентном выборе продукции, работ, услуг;

– повышение конкурентоспособности продукции, работ, услуг на российском и международном рынках;

– создание условий для обеспечения свободного перемещения товаров по территории Российской Федерации, а также для осуществления международного экономического, научно-технического сотрудничества и международной торговли.

Подтверждение соответствия осуществляется на основе следующих принципов:

– доступности информации о порядке осуществления подтверждения соответствия заинтересованным лицам;

– недопустимости применения обязательного подтверждения соответствия к объектам, в отношении которых не установлены требования технических регламентов;

– установления перечня форм и схем обязательного подтверждения соответствия в отношении определенных видов продукции в соответствующем техническом регламенте;

– уменьшения сроков осуществления обязательного подтверждения соответствия и затрат заявителя;

– недопустимости принуждения к осуществлению добровольного подтверждения соответствия, в том числе в определенной системе добровольной сертификации;

– защиты имущественных интересов заявителей, соблюдения коммерческой тайны в отношении сведений, полученных при осуществлении подтверждения соответствия;

– недопустимости подмены обязательного подтверждения соответствия добровольной сертификацией.

Подтверждение соответствия на территории Российской Федерации может носить добровольный или обязательный характер.

Добровольное подтверждение соответствия осуществляется в форме добровольной сертификации, осуществляемой по инициативе заявителя на условиях договора между заявителем и органом по сертификации, для установления соответствия национальным стандартам, стандартам организаций, системам добровольной сертификации, условиям договоров.

Объектами добровольного подтверждения соответствия являются продукция, процессы производства, эксплуатации, хранения, перевозки, реализации и утилизации, работы и услуги, а также объекты, в отношении которых стандартами, системами добровольной сертификации и договорами устанавливаются требования.

Система добровольной сертификации может быть создана юридическим лицом и (или) индивидуальным предпринимателем или несколькими юридическими лицами и (или) индивидуальными предпринимателями.

Лицо или лица, создавшие систему добровольной сертификации, устанавливают перечень объектов, подлежащих сертификации, и их характеристик, на соответствие которым осуществляется добровольная сертификация, правила выполнения предусмотренных данной системой добровольной сертификации работ и порядок их оплаты, определяют участников данной системы добровольной сертификации. Системой добровольной сертификации может предусматриваться применение знака соответствия.

Объекты сертификации, сертифицированные в системе добровольной сертификации, могут маркироваться знаком соответствия системы добровольной сертификации. Порядок применения такого знака соответствия устанавливается правилами соответствующей системы добровольной сертификации.

Применение знака соответствия национальному стандарту осуществляется заявителем на добровольной основе любым удобным для заявителя способом в порядке, установленном национальным органом по стандартизации.

Обязательное подтверждение соответствия проводится только в случаях, установленных соответствующим техническим регламентом, и исключительно на соответствие требованиям технического регламента и осуществляется в формах: принятия декларации о соответствии; обязательной сертификации.

Объектом обязательного подтверждения соответствия может быть только продукция, выпускаемая в обращение на территории Российской Федерации.

Форма и схемы обязательного подтверждения соответствия могут устанавливаться только техническим регламентом с учетом степени риска недостижения целей технических регламентов.

Декларация о соответствии и сертификат соответствия имеют равную юридическую силу независимо от схем обязательного подтверждения соответствия и действуют на всей территории Российской Федерации.

Декларирование соответствия осуществляется по одной из следующих схем:

– принятие декларации о соответствии на основании собственных доказательств;

– принятие декларации о соответствии на основании собственных доказательств, доказательств, полученных с участием органа по сертификации и (или) аккредитованной испытательной лаборатории (центра) (далее — третья сторона).

При декларировании соответствия заявителем могут быть зарегистрированные в соответствии с законодательством Российской Федерации на ее территории юридическое или физическое лицо в качестве индивидуального предпринимателя, либо являющиеся изготовителем или продавцом, либо выполняющие функции иностранного изготовителя на основании договора с ним в части обеспечения соответствия поставляемой продукции требованиям технических регламентов и в части ответственности за несоответствие поставляемой продукции требованиям технических регламентов (лицо, выполняющее функции иностранного изготовителя).

Круг заявителей устанавливается соответствующим техническим регламентом.

При декларировании соответствия на основании собственных доказательств заявитель самостоятельно формирует доказательственные материалы в целях подтверждения соответствия продукции требованиям технических регламентов. В качестве доказательственных материалов используются техническая документация, результаты собственных исследований (испытаний) и измерений и (или) другие документы, послужившие мотивированным основанием для подтверждения соответствия продукции требованиям технических регламентов. Состав доказательственных материалов определяется соответствующим техническим регламентом.

Сертификат системы качества может использоваться в составе доказательств при принятии декларации о соответствии любой продукции, за исключением случая, если для такой продукции техническими регламентами предусмотрена иная форма подтверждения соответствия.

Обязательная сертификация осуществляется органом по сертификации на основании договора с заявителем. Схемы сертификации, применяемые для сертификации определенных видов про-

дукции, устанавливаются соответствующим техническим регламентом.

Соответствие продукции требованиям технических регламентов подтверждается сертификатом соответствия, выдаваемым заявителю органом по сертификации.

Обязательная сертификация осуществляется органом по сертификации, аккредитованным в порядке, установленном Правительством Российской Федерации.

Федеральный орган исполнительной власти по техническому регулированию ведет единый реестр выданных сертификатов соответствия.

Порядок ведения единого реестра выданных сертификатов соответствия, порядок предоставления содержащихся в едином реестре сведений и порядок оплаты за предоставление содержащихся в указанном реестре сведений устанавливаются Правительством Российской Федерации.

Исследования (испытания) и измерения продукции при осуществлении обязательной сертификации проводятся *аккредитованными испытательными лабораториями (центрами)*.

Аккредитованные испытательные лаборатории (центры) проводят исследования (испытания) и измерения продукции в пределах своей области аккредитации на условиях договоров с органами по сертификации. Органы по сертификации не вправе предоставлять аккредитованным испытательным лабораториям (центрам) сведения о заявителе.

13.5. Информация о нарушении требований технических регламентов и стандартов

За нарушение требований технических регламентов изготовитель (исполнитель, продавец, лицо, выполняющее функции иностранного изготовителя) несет ответственность в соответствии с законодательством Российской Федерации.

В случае, если в результате несоответствия продукции требованиям технических регламентов, нарушений требований технических регламентов при осуществлении процессов производства, эксплуатации, хранения, перевозки, реализации и утилизации причинен вред жизни или здоровью граждан, имуществу физических или юридических лиц, государственному или муниципальному имуществу, окружающей среде, жизни или здоровью животных и растений или возникла угроза причинения такого вреда, ***изготовитель (исполнитель, продавец, лицо, выполняющее функции иностранного изготовителя) обязан возместить причиненный вред*** и принять меры в целях недопущения причинения вреда другим лицам, их имуществу, окружающей среде в соответствии с законодательством Российской Федерации.

Обязанность возместить вред не может быть ограничена договором или заявлением одной из сторон. Соглашения или заявления об ограничении ответственности ничтожны.

Изготовитель (исполнитель, продавец, лицо, выполняющее функции иностранного изготовителя), которому стало известно о несоответствии выпущенной в обращение продукции требованиям технических регламентов, обязан сообщить об этом в орган государственного контроля (надзора) в соответствии с его компетенцией в течение десяти дней с момента получения указанной информации.

Продавец (исполнитель, лицо, выполняющее функции иностранного изготовителя), получивший указанную информацию, в течение десяти дней обязан довести ее до изготовителя.

Лицо, которое не является изготовителем (исполнителем, продавцом, лицом, выполняющим функции иностранного изготовителя) и которому стало известно о несоответствии выпущенной в обращение продукции требованиям технических регламентов, вправе направить информацию о несоответствии продукции требованиям технических регламентов в орган государственного контроля (надзора).

При получении такой информации орган государственного контроля (надзора) в течение пяти дней обязан известить изготовителя (продавца, лицо, выполняющее функции иностранного изготовителя) о ее поступлении.

В течение десяти дней с момента получения информации о несоответствии продукции требованиям технических регламентов, если необходимость установления более длительного срока не следует из существа проводимых мероприятий, изготовитель (продавец, лицо, выполняющее функции иностранного изготовителя) обязан провести проверку достоверности полученной информации. По требованию органа государственного контроля (надзора) изготовитель (продавец, лицо, выполняющее функции иностранного изготовителя) обязан представить материалы указанной проверки в орган государственного контроля (надзора).

В случае получения информации о несоответствии продукции требованиям технических регламентов изготовитель (продавец, лицо, выполняющее функции иностранного изготовителя) обязан принять необходимые меры для того, чтобы до завершения проверки, предусмотренной абзацем первым настоящего пункта, возможный вред, связанный с обращением данной продукции, не увеличился.

При подтверждении достоверности информации о несоответствии продукции требованиям технических регламентов изготовитель (продавец, лицо, выполняющее функции иностранного изготовителя) в течение десяти дней с момента подтверждения достоверно-

сти такой информации обязан разработать программу мероприятий по предотвращению причинения вреда и согласовать ее с органом государственного контроля (надзора) в соответствии с его компетенцией.

Программа должна включать мероприятия по оповещению приобретателей о наличии угрозы причинения вреда и способах его предотвращения, а также сроки реализации этих мероприятий.

В случае, если для предотвращения причинения вреда необходимо произвести дополнительные расходы, изготовитель (продавец, лицо, выполняющее функции иностранного изготовителя) обязан осуществить все мероприятия по предотвращению причинения вреда своими силами, а при невозможности их осуществления объявить об отзыве продукции и возместить убытки, причиненные приобретателям в связи с отзывом продукции.

Устранение недостатков, а также доставка продукции к месту устранения недостатков и возврат ее приобретателям осуществляются изготовителем (продавцом, лицом, выполняющим функции иностранного изготовителя) и за его счет.

В случае, если угроза причинения вреда не может быть устранена путем проведения указанных выше мероприятий, изготовитель (продавец, лицо, выполняющее функции иностранного изготовителя) обязан незамедлительно приостановить производство и реализацию продукции, отозвать продукцию и возместить приобретателям убытки, возникшие в связи с отзывом продукции.

На весь период действия программы мероприятий по предотвращению причинения вреда изготовитель (продавец, лицо, выполняющее функции иностранного изготовителя) за свой счет обязан обеспечить приобретателям возможность получения оперативной информации о необходимых действиях.

Органы государственного контроля (надзора) в случае получения информации о несоответствии продукции требованиям технических регламентов в возможно короткие сроки проводят проверку достоверности полученной информации.

При признании достоверности информации о несоответствии продукции требованиям технических регламентов орган государственного контроля (надзора) в соответствии с его компетенцией в течение десяти дней выдает предписание о разработке изготовителем (продавцом, лицом, выполняющим функции иностранного изготовителя) программы мероприятий по предотвращению причинения вреда, оказывает содействие в ее реализации и осуществляет контроль за ее выполнением.

В случае невыполнения предписания или невыполнения программы мероприятий по предотвращению причинения вреда орган государственного контроля (надзора) в соответствии с его компетенцией, а также иные лица, которым стало известно о невыполнении

изготовителем (продавцом, лицом, выполняющим функции иностранного изготовителя) программы мероприятий по предотвращению причинения вреда, вправе обратиться в суд с иском о принудительном отзыве продукции.

В случае удовлетворения иска о принудительном отзыве продукции суд обязывает ответчика совершить определенные действия, связанные с отзывом продукции, в установленный судом срок, а также довести решение суда не позднее одного месяца со дня его вступления в законную силу до сведения приобретателей через средства массовой информации или иным способом.

В случае, если ответчик не исполнит решение суда в установленный срок, истец вправе совершить эти действия за счет ответчика с взысканием с него необходимых расходов.

За нарушение требований законодательства об отзыве продукции могут быть применены меры уголовного и административного воздействия в соответствии с законодательством Российской Федерации.

Национальные стандарты и общероссийские классификаторы, а также информация об их разработке должны быть доступны заинтересованным лицам.

Официальное опубликование в установленном порядке национальных стандартов и общероссийских классификаторов осуществляется национальным органом по стандартизации. Порядок опубликования национальных стандартов и общероссийских классификаторов определяется Правительством Российской Федерации.

Технические регламенты, документы национальной системы стандартизации, международные стандарты, правила стандартизации, нормы стандартизации и рекомендации по стандартизации, национальные стандарты других государств и информация о международных договорах в области стандартизации и подтверждения соответствия и о правилах их применения составляют *Федеральный информационный фонд технических регламентов и стандартов.*

Федеральный информационный фонд технических регламентов и стандартов является *государственным информационным ресурсом.*

В Российской Федерации в порядке и на условиях, которые установлены Правительством Российской Федерации, создается и функционирует единая информационная система, предназначенная для обеспечения заинтересованных лиц информацией о документах, входящих в состав Федерального информационного фонда технических регламентов и стандартов.

Заинтересованным лицам обеспечивается свободный доступ к создаваемым информационным ресурсам, за исключением случаев, если в интересах сохранения государственной, служебной или коммерческой тайны такой доступ должен быть ограничен.

Контрольные вопросы

1. Перечислите основные источники права в области технического регулирования.
2. Раскройте понятие «технические регламенты», содержание регламентов и предметную область действия.
3. Перечислите виды технических регламентов.
4. Раскройте содержание понятия «стандарт», виды стандартов и цели принятия.
5. Каков механизм подтверждения соответствия техническим регламентам и стандартам?
6. Каков механизм обеспечения соблюдения требований технических регламентов и стандартов?

Глава 14

ЮРИДИЧЕСКАЯ ОТВЕТСТВЕННОСТЬ

14.1. Общие положения

Юридической ответственностью называется применение к лицу, совершившему правонарушение, мер государственного принуждения, предусмотренных санкцией нарушенной нормы, в установленном для этого процессуальном порядке.

Общей целью применения юридической ответственности является охрана правопорядка. Эта цель в зависимости от характера правонарушений и их последствий достигается либо принудительным восстановлением нарушенных прав и пресечением противоправных состояний, либо наказанием правонарушителя, либо сочетанием того и другого.

Основанием ответственности является правонарушение (действительное или предполагаемое), которое характеризуется четырьмя элементами, образующими состав правонарушения:

– *объект* — нарушенное материальное или нематериальное благо, защищаемое правом;

– *субъект* — дееспособное лицо, совершившее правонарушение;

– *объективная сторона* — само противоправное деяние, наступивший вредоносный результат и причинная связь между деянием и результатом;

– *субъективная сторона* — вина, т.е. отношение правонарушителя к деянию и его результату в форме умысла или неосторожности.

Юридическая ответственность может быть возложена на лицо лишь при установлении всех элементов состава правонарушения. Это требование является обязательным при возложении дисциплинарной, административной и уголовной ответственности. По гражданским правонарушениям правонарушитель при определенных обстоятельствах может нести ответственность и без вины.

При применении к лицу мер государственного принуждения карательного характера (в административном и уголовном праве) действует *принцип презумпции невиновности*, т.е. предположение, в соответствии с которым даже при наличии фактов, свидетельствующих в доказанности объективной стороны, лицо считается невиновным, пока в предусмотренном законом порядке не будет

доказана и установлена судом его вина. При этом бремя доказывания лежит на компетентных государственных органах — органах следствия, прокуратуре, осуществляющих обвинение.

Ответственность всегда конкретна: это ответственность определенного лица за доказуемое нарушение точно обозначенной нормы права при обстоятельствах, заранее предусмотренных законом или другими нормативными актами.

Правонарушение не причиняет урона и ущерба нормам закона, которые продолжают действовать и считаются обязательными; оно вредно или опасно для общества, стабильности общественных отношений, конкретных прав и охраняемых законом интересов.

Правонарушение представляет собой конкретный факт, юридическое определение (квалификация) которого содержится в законе. То же и правовое принуждение: оно может применяться лишь к конкретным лицам (субъектам права) за точно определенные нарушения в той сфере, где люди общаются между собой, вступают в отношения.

Применение юридической ответственности осуществляется на основе нормативных конструкций, представляющих *единство норм материального и процессуального права.*

Признаки правонарушения и санкции за его совершение предусмотрены нормами материального права; порядок доказывания, определения того, было или не было правонарушение и кто его совершил, а также назначение конкретной меры государственного принуждения в пределах санкции нарушенной нормы строго регламентированы нормами процессуального права.

Основные виды юридической ответственности предопределяются содержанием санкций, которые применяются за правонарушения.

Санкции делятся на два основных вида в соответствии со способом, каким они служат охране правопорядка:

– *правовосстановительные санкции*, которые направлены на устранение непосредственного вреда, причиненного правопорядку (восстановление нарушенных прав, принудительное выполнение обязанностей, устранение противоправных состояний);

– *штрафные, карательные санкции*, которые имеют целью воздействие на правонарушителя в целях общей и частной превенции правонарушений (дисциплинарные, административные и уголовно-правовые санкции).

Поскольку выраженный в санкции способ охраны правопорядка предопределяет порядок ее применения и реализации, соответственно и основным делением видов ответственности является деление на правовосстановительную и штрафную.

Для *правовосстановительной ответственности* существенно важно точное определение уже существующих обязанностей пра-

вонарушителя и в случае необходимости их принудительное осуществление. Для *штрафной, карательной ответственности* — правильная квалификация правонарушения, индивидуализация наказания или взыскания, реализация примененных к правонарушителю мер принуждения, освобождение его от ответственности, когда ее цели достигнуты. К штрафной, карательной ответственности, сообразно видам правонарушений и санкций за их совершение, относятся уголовная, административная и дисциплинарная ответственность.

В процессе *применения юридической ответственности* могут применяться предусмотренные законодательством принудительные меры, обеспечивающие производство по делу о правонарушении — меры обеспечения доказательств (обыски, выемки и др.) или исполнения решения (опись имущества, его изъятие и др.), а также меры пресечения (отстранение от работы, задержание, содержание под стражей и др.). Эти принудительные меры носят вспомогательный характер: их применение зависит от тяжести правонарушения, но не содержит его итоговой правовой оценки (их применением не исчерпывается и не решается вопрос об ответственности за правонарушение); при применении санкции они поглощаются назначенным наказанием, взысканием, принудительным исполнением.

При юридической ответственности нарушитель претерпевает меры государственного принуждения за свою вину и несет известные лишения, урон.

14.2. Правовосстановительная ответственность

Правовосстановительная ответственность, как правило, применяется при нарушении правовых норм, регулирующих гражданские отношения, и заключается в восстановлении незаконно нарушенных прав, в принудительном исполнении невыполненной обязанности. Основным источником права в этой области является Гражданский кодекс Российской Федерации.

Особенность этого вида ответственности состоит в том, что в ряде случаев правонарушитель может без вмешательства государственных органов выполнить свои обязанности, восстановить нарушенные права, прекратить противоправное состояние. На этом основаны дополнительные санкции, применяемые к правонарушителю в процессе реализации данных отношений ответственности (пени, штрафы, другие меры понуждения).

Так, в соответствии с Гражданским кодексом лица, незаконными методами получившие информацию, которая составляет коммерческую тайну, обязаны возместить причиненные убытки. Такая же обязанность возлагается на работников, разгласивших коммерческую тайну вопреки трудовому договору, в том числе

контракту, и на контрагентов, сделавших это вопреки гражданско-правовому договору.

Если гражданину причинен моральный вред (физические или нравственные страдания) действиями, нарушающими его личные неимущественные права либо посягающими на принадлежащие другие нематериальные блага, а также в других случаях, предусмотренных законом, суд может возложить на нарушителя обязанность денежной компенсации указанного вреда.

Гражданин вправе требовать по суду опровержения порочащих его честь, достоинство или деловую репутацию сведений, если распространивший эти сведения не докажет, что они соответствуют действительности. Кроме того, он вправе наряду с опровержением требовать возмещения убытков и морального вреда, причиненного распространением таких сведений.

Если сведения, порочащие честь, достоинство или деловую репутацию гражданина, распространены в средствах массовой информации, то они должны быть опровергнуты в тех же средствах массовой информации.

Правовосстановительная ответственность возникает с момента правонарушения и завершается восстановлением (в установленных законом пределах) нарушенного правопорядка. Процессуальные нормы регулируют осуществление этого вида ответственности в случае спора (в суде, в арбитраже) или отказа правонарушителя восстановить нарушенный правопорядок (исполнительное производство).

14.3. Дисциплинарная и административная ответственность

Дисциплинарная ответственность применяется за нарушение трудовой, учебной, служебной, воинской дисциплины. Рабочие и служащие, нарушившие трудовую дисциплину, привлекаются к дисциплинарной ответственности администрацией предприятия, учреждения, организации. До наложения взыскания должны быть затребованы объяснения от нарушителя трудовой дисциплины. Законодательством определен порядок обжалования дисциплинарного взыскания, сроки его применения и действия, порядок досрочного снятия. Определенную специфику имеет дисциплинарная ответственность работников гражданской авиации, железнодорожного транспорта, военнослужащих по уставам о дисциплине, а также дисциплинарная ответственность судей и некоторых других категорий должностных лиц, дела о проступках которых рассматриваются и решаются специальными дисциплинарными коллегиями.

Административная ответственность осуществляется на основе законодательства об административных правонарушениях. Это законодательство состоит из Кодекса Российской Федерации об административных правонарушениях.

Основными задачами законодательства об административных правонарушениях являются защита личности, охрана прав и свобод человека и гражданина, охрана здоровья граждан, санитарно-эпидемиологического благополучия населения, защита общественной нравственности, охрана окружающей среды, установленного порядка осуществления государственной власти, общественного порядка и общественной безопасности, собственности, защита законных интересов физических и юридических лиц, общества и государства от административных правонарушений, а также их предупреждение.

Административным правонарушением признается противоправное, виновное действие (бездействие) физического или юридического лица, за которое Кодексом Российской Федерации об административных правонарушениях установлена административная ответственность.

Административная ответственность проявляется в форме административного наказания. Установлены следующие *виды административных наказаний*: предупреждение; административный штраф; возмездное изъятие орудия совершения или предмета административного правонарушения; конфискация орудия совершения или предмета административного правонарушения; лишение специального права, предоставленного физическому лицу; административный арест; административное выдворение за пределы Российской Федерации иностранного гражданина или лица без гражданства; дисквалификация.

Законодательство об административных правонарушениях закрепляет значительное количество правонарушений в области информационной безопасности, за совершение которых к виновным лицам должна применяться административная ответственность.

Так, *ввоз, продажа, сдача в прокат или иное незаконное использование экземпляров произведений или фонограмм в целях извлечения дохода в случаях, если экземпляры произведений или фонограмм являются контрафактными в соответствии с законодательством Российской Федерации об авторском праве и смежных правах, либо на экземплярах произведений или фонограмм указана ложная информация об изготовителях, о местах их производства, а также об обладателях авторских и смежных прав, а равно иное нарушение авторских и смежных прав в целях извлечения дохода* влечет наложение административного штрафа с конфискацией контрафактных экземпляров произведений и фонограмм, а также материалов и оборудования, используемых для их произведения, и иных орудий совершения административного правонарушения на граждан в размере от пятнадцати до двадцати минимальных размеров оплаты труда; на должностных лиц — от тридцати до сорока минимальных размеров оплаты труда; на юридических лиц — от трехсот до четырехсот минимальных размеров оплаты труд.

Незаконное использование изобретения, полезной модели либо промышленного образца, разглашение без согласия автора или заявителя сущности изобретения, полезной модели либо промышленного образца до официального опубликования сведений о них, присвоение авторства или принуждение к соавторству влечет наложение административного штрафа на граждан в размере от пятнадцати до двадцати минимальных размеров оплаты труда; на юридических лиц — от трехсот до четырехсот минимальных размеров оплаты труда.

Нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных) влечет предупреждение или наложение административного штрафа на граждан в размере от трех до пяти минимальных размеров оплаты труда; на должностных лиц — от пяти до десяти минимальных размеров оплаты труда; на юридических лиц — от пятидесяти до ста минимальных размеров оплаты труда.

Нарушение условий, предусмотренных лицензией на осуществление деятельности в области защиты информации (за исключением информации, составляющей государственную тайну), влечет наложение административного штрафа на граждан в размере от трех до пяти минимальных размеров оплаты труда; на должностных лиц — от пяти до десяти минимальных размеров оплаты труда; на юридических лиц — от пятидесяти до ста минимальных размеров оплаты труда.

Использование несертифицированных информационных систем, баз и банков данных, а также несертифицированных средств защиты информации, если они подлежат обязательной сертификации (за исключением средств защиты информации, составляющей государственную тайну), влечет наложение административного штрафа на граждан в размере от пяти до десяти минимальных размеров оплаты труда с конфискацией несертифицированных средств защиты информации или без таковой; на должностных лиц — от десяти до двадцати минимальных размеров оплаты труда; на юридических лиц — от ста до двухсот минимальных размеров оплаты труда с конфискацией несертифицированных средств защиты информации или без таковой.

Нарушение условий, предусмотренных лицензией на проведение работ, связанных с использованием и защитой информации, составляющей государственную тайну, созданием средств, предназначенных для защиты информации, составляющей государственную тайну, осуществлением мероприятий и (или) оказанием услуг по защите информации, составляющей государственную тайну, влечет наложение административного штрафа на должностных лиц в размере от двадцати до тридцати минимальных размеров оплаты труда; на юридических лиц — от ста пятидесяти до двухсот минимальных размеров оплаты труда.

Использование несертифицированных средств, предназначенных для защиты информации, составляющей государственную тайну, влечет наложение административного штрафа на должностных лиц в размере от тридцати до сорока минимальных размеров оплаты труда с конфискацией несертифицированных средств, предназначенных для защиты информации, составляющей государственную тайну, или без таковой.

Разглашение информации, доступ к которой ограничен федеральным законом (за исключением случаев, если разглашение такой информации влечет уголовную ответственность), лицом, получившим доступ к такой информации в связи с исполнением служебных или профессиональных обязанностей, влечет наложение административного штрафа на граждан в размере от пяти до десяти минимальных размеров оплаты труда; на должностных лиц — от сорока до пятидесяти минимальных размеров оплаты труда.

Производство по делу начинается с составления протокола об административном правонарушении. В предусмотренных законом случаях к лицу, привлеченному к административной ответственности, могут применяться меры обеспечения производства по делу: административное задержание лица, личный досмотр, досмотр вещей и изъятие вещей и документов. Дела об административных нарушениях рассматриваются народными судами, народными судьями, органами внутренних дел, органами государственных инспекций и другими государственными органами и должностными лицами, уполномоченными на то законодательными актами. Дело рассматривается открыто, в присутствии лица, привлекаемого к административной ответственности. Привлеченный к ответственности вправе знакомиться с материалами дела, давать объяснения, представлять доказательства, заявлять ходатайства, пользоваться юридической помощью адвоката, обжаловать постановление по делу; он также имеет ряд других прав. Законодательством определены сроки привлечения к административной ответственности и исполнения наложенных взысканий.

14.4. Уголовная ответственность

Уголовная ответственность применяется за преступления и включает самые строгие меры государственного принуждения. Порядок ее осуществления регламентирован наиболее детально и определяется уголовным, уголовно-процессуальным и уголовно-исполнительным законодательством. Ряд принципов уголовной ответственности закреплен в международных пактах и в конституционном законодательстве.

Уголовное законодательство составляет Уголовный кодекс Российской Федерации.

Задачами уголовного законодательства являются охрана прав и свобод человека и гражданина, собственности, общественного порядка и общественной безопасности, окружающей среды, конституционного строя Российской Федерации от преступных посягательств, обеспечение мира и безопасности человечества, а также предупреждение преступлений.

Преступлением признается виновно совершенное общественно опасное деяние, запрещенное Уголовным кодексом Российской Федерации под угрозой наказания.

Не является преступлением действие (бездействие), хотя формально и содержащее признаки какого-либо деяния, предусмотренного кодексом, но в силу малозначительности не представляющее общественной опасности.

В зависимости от характера и степени общественной опасности деяния, предусмотренные Уголовным кодексом, подразделяются на преступления небольшой тяжести, средней тяжести, тяжкие и особо тяжкие.

Физическое лицо подлежит уголовной ответственности только за те общественно опасные действия (бездействие) и наступившие общественно опасные последствия, в отношении которых установлена его вина.

Наказание и иные меры уголовно-правового характера, применяемые к лицу, совершившему преступление, должны быть справедливыми, т.е. соответствовать характеру и степени общественной опасности преступления, обстоятельствам его совершения и личности виновного.

Виновным в преступлении признается лицо, совершившее деяние умышленно или по неосторожности. Деяние, совершенное только по неосторожности, признается преступлением лишь в случае, когда это специально предусмотрено соответствующей статьей Уголовного кодекса.

Уголовная ответственность проявляется в форме наказания. *Наказание* есть мера государственного принуждения, назначаемая по приговору суда. Наказание применяется к лицу, признанному виновным в совершении преступления, и заключается в предусмотренных Уголовным кодексом лишении или ограничении прав и свобод этого лица. Оно применяется в целях восстановления социальной справедливости, а также в целях исправления осужденного и предупреждения совершения новых преступлений.

Видами наказаний являются: штраф; лишение права занимать определенные должности или заниматься определенной деятельностью; лишение специального, воинского или почетного звания, классного чина и государственных наград; обязательные работы; исправительные работы; ограничение по военной службе; ограничение свободы; арест; содержание в дисциплинарной во-

инской части; лишение свободы на определенный срок; пожизненное лишение свободы; смертная казнь.

В уголовном законодательстве содержится значительное количество общественно опасных деяний в информационной сфере. Часть этих деяний связана со сферой компьютерной информации, которая в рамках данного раздела представляет наибольший интерес.

К числу этих деяний относятся следующие.

Неправомерный доступ к охраняемой законом компьютерной информации, т.е. информации на машинном носителе, в электронно-вычислительной машине (ЭВМ), системе ЭВМ или их сети, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети, наказывается штрафом в размере до 200 тыс. р. или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо исправительными работами на срок от шести месяцев до одного года, либо лишением свободы на срок до двух лет.

То же деяние, совершенное группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения, а равно имеющим доступ к ЭВМ, системе ЭВМ или их сети, наказывается штрафом в размере от 100 тыс. до 300 тыс. р. или в размере заработной платы или иного дохода осужденного за период от одного года до двух лет, либо исправительными работами на срок от одного года до двух лет, либо арестом на срок от трех до шести месяцев, либо лишением свободы на срок до пяти лет.

Создание программ для ЭВМ или внесение изменений в существующие программы, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети, а равно использование либо распространение таких программ или машинных носителей с такими программами наказываются лишением свободы на срок до трех лет со штрафом в размере до 200 тыс. р. или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев.

Те же деяния, повлекшие по неосторожности тяжкие последствия, наказываются лишением свободы на срок от трех до семи лет.

Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети лицом, имеющим доступ к ЭВМ, системе ЭВМ или их сети, повлекшее уничтожение, блокирование или модификацию охраняемой законом информации ЭВМ, если это деяние причинило существенный вред, наказывается лишением права занимать определенные должности или заниматься определенной деятельностью на срок до пяти лет, либо обязательными работами на срок от 180 до 240 ч, либо ограничением свободы на срок до двух лет.

То же деяние, повлекшее по неосторожности тяжкие последствия, наказывается лишением свободы на срок до четырех лет.

Привлечению определенного лица к уголовной ответственности в качестве обвиняемого обычно предшествует возбуждение уголовного дела по факту преступления, сбор и исследование относящихся к этому делу доказательств. С момента привлечения к уголовной ответственности обвиняемый имеет право на защиту. Уголовно-процессуальным законодательством определены права и обязанности обвиняемого, подозреваемого и других участников процесса, а также правомочия должностных лиц и государственных органов, ведающих производством по делу, порядок сбора и исследования доказательств, применения в случае необходимости принудительных мер (мер пресечения, обысков, выемок, приводов и др.). Решающей стадией уголовной ответственности является рассмотрение дела в судебном заседании. Никто не может быть признан виновным в совершении преступления, а также подвергнут уголовному наказанию иначе как по приговору суда и в соответствии с законом. Каждый осужденный за уголовное преступление имеет право на пересмотр приговора вышестоящей судебной инстанцией в порядке, установленном законом, а также право просить о помиловании или смягчении наказания.

Отношения уголовной ответственности завершаются отбытием наказания, назначенного осужденному.

Контрольные вопросы

1. В чем заключается применение юридической ответственности? Раскройте ее сущность и признаки.
2. В чем заключается правоприменительная ответственность?
3. В чем заключается дисциплинарная и административная ответственность?
4. В чем заключается уголовная ответственность?

Глава 15

ЗАЩИТА ПРАВ И ЗАКОННЫХ ИНТЕРЕСОВ СУБЪЕКТОВ ИНФОРМАЦИОННОЙ СФЕРЫ

15.1. Суды общей юрисдикции, арбитражные суды и третейские суды

Одним из наиболее важных способов защиты прав и законных интересов субъектов информационной сферы является *судебное разбирательство*, осуществляемое в рамках деятельности *судебной власти*.

Судебная власть представляет собой самостоятельную и независимую составляющую государственной власти, действующую наряду с законодательной и исполнительной властями.

Судебная система Российской Федерации образуется совокупностью федеральных судов, конституционных (уставных) судов и мировых судей субъектов Российской Федерации

К *федеральным судам* относятся:

– Конституционный Суд Российской Федерации;

– суды общей юрисдикции — Верховный Суд Российской Федерации, верховные суды республик, краевые и областные суды, суды городов федерального значения, суды автономной области и автономных округов, районные суды, военные и специализированные суды, составляющие систему федеральных судов общей юрисдикции;

– арбитражные суды — Высший Арбитражный Суд Российской Федерации, федеральные арбитражные суды округов (арбитражные кассационные суды), арбитражные апелляционные суды, арбитражные суды субъектов Российской Федерации, составляющие систему федеральных арбитражных судов.

К *судам субъектов Российской Федерации* относятся:

– конституционные (уставные) суды субъектов Российской Федерации, мировые судьи, являющиеся судьями общей юрисдикции субъектов Российской Федерации.

Конституционный Суд Российской Федерации является судебным органом конституционного контроля, самостоятельно и независимо осуществляющим судебную власть посредством конституционного судопроизводства.

Верховный Суд Российской Федерации является высшим судебным органом по гражданским, уголовным, административным и иным делам, подсудным судам общей юрисдикции. Он осуществляет в предусмотренных федеральным законом процессуальных формах судебный надзор за деятельностью судов общей юрисдик-

ции, включая военные и специализированные федеральные суды. В пределах своей компетенции Верховный Суд Российской Федерации рассматривает дела в качестве суда второй инстанции, в порядке надзора и по вновь открывшимся обстоятельствам, а в случаях, предусмотренных федеральным законом, также и в качестве суда первой инстанции.

Верховный Суд Российской Федерации является непосредственно вышестоящей судебной инстанцией по отношению к верховным судам республик, краевым (областным) судам, судам городов федерального значения, судам автономной области и автономных округов, военным судам военных округов, флотов, видов и групп войск. Он уполномочен давать разъяснения по вопросам судебной практики.

Верховный суд республики, краевой (областной) суд, суд города федерального значения, суд автономной области, суд автономного округа в пределах своей компетенции рассматривают дела в качестве суда первой и второй инстанции, в порядке надзора и по вновь открывшимся обстоятельствам. Эти суды являются непосредственно вышестоящими судебными инстанциями по отношению к районным судам, действующим на территории соответствующего субъекта Российской Федерации.

Районный суд в пределах своей компетенции рассматривает дела в качестве суда первой и второй инстанции и осуществляет другие полномочия, предусмотренные федеральным конституционным законом. Районный суд является непосредственно вышестоящей судебной инстанцией по отношению к мировым судьям, действующим на территории соответствующего судебного района.

Военные суды создаются по территориальному принципу по месту дислокации войск и флотов и осуществляют судебную власть в войсках, органах и формированиях, где федеральным законом предусмотрена военная служба. В пределах своей компетенции военные суды рассматривают дела в качестве суда первой и второй инстанции, в порядке надзора и по вновь открывшимся обстоятельствам.

Высший Арбитражный Суд Российской Федерации является высшим судебным органом по разрешению экономических споров и иных дел, рассматриваемых арбитражными судами. Он является вышестоящей судебной инстанцией по отношению к федеральным арбитражным судам округов, арбитражным апелляционным судам и арбитражным судам субъектов Российской Федерации.

Высший Арбитражный Суд Российской Федерации осуществляет в предусмотренных федеральным законом процессуальных формах судебный надзор за деятельностью арбитражных судов, рассматривает в соответствии с федеральным законом дела в качестве суда первой инстанции, в порядке надзора и по вновь открывшимся обстоятельствам.

Высший Арбитражный Суд Российской Федерации уполномочен давать разъяснения по вопросам судебной практики.

Федеральный арбитражный суд округа в пределах своей компетенции рассматривает дела в качестве суда кассационной инстанции, а также по вновь открывшимся обстоятельствам. Он является вышестоящей судебной инстанцией по отношению к действующим на территории соответствующего судебного округа арбитражным апелляционным судам и арбитражным судам субъектов Российской Федерации.

Арбитражный апелляционный суд в пределах своей компетенции рассматривает дела в качестве суда апелляционной инстанции, а также по вновь открывшимся обстоятельствам.

Арбитражный суд субъекта Российской Федерации в пределах своей компетенции рассматривает дела в качестве суда первой инстанции, а также по вновь открывшимся обстоятельствам.

Специализированные федеральные суды по рассмотрению гражданских и административных дел учреждаются путем внесения изменений и дополнений в настоящий Федеральный конституционный закон.

Конституционный (уставный) суд субъекта Российской Федерации может создаваться субъектом Российской Федерации для рассмотрения вопросов соответствия законов субъекта Российской Федерации, нормативных правовых актов органов государственной власти субъекта Российской Федерации, органов местного самоуправления субъекта Российской Федерации конституции (уставу) субъекта Российской Федерации, а также для толкования конституции (устава) субъекта Российской Федерации. Конституционный (уставный) суд субъекта Российской Федерации рассматривает отнесенные к его компетенции вопросы в порядке, установленном законом субъекта Российской Федерации. Решение, принятое им в пределах установленных полномочий, не может быть пересмотрено иным судом.

Мировой судья в пределах своей компетенции рассматривает гражданские, административные и уголовные дела в качестве суда первой инстанции.

Суд представляет собой государственный орган, осуществляющий правосудие в форме рассмотрения и разрешения уголовных, гражданских, административных и некоторых иных категорий дел в установленном законодательством процессуальном порядке.

Суды осуществляют судебную власть самостоятельно, независимо от чьей бы то ни было воли, подчиняясь только Конституции Российской Федерации и закону.

Судьи, присяжные, народные и арбитражные заседатели, участвующие в осуществлении правосудия, независимы и подчиняются только Конституции Российской Федерации и закону. Гарантии их независимости устанавливаются Конституцией Российской Федерации и федеральным законом.

Защиту прав и законных интересов граждан и организаций можно осуществлять в *третейских судах*, если существует соглашение сторон о передаче дела в третейский суд. Соглашение заключается в письменной форме. Стороны, передавая спор на рассмотрение третейского суда, принимают обязательство подчиниться решению последнего. Третейские суды не входят в судебную систему. Деятельность третейских судов регулируется законом «О третейских судах в Российской Федерации» от 21 июня 2002 г., а также отдельными положениями гражданского и арбитражного процессуального законодательства.

Действующие в качестве негосударственного механизма разрешения споров, третейские суды, по сравнению с судами арбитражными, предоставляют участникам спора ряд преимуществ, таких, как специализация в вопросах, касающихся фактических взаимоотношений сторон, быстрота и экономичность, отсутствие публичности в деятельности, удобство для сторон в отношении времени и места разрешения споров и т.д.

В Российской Федерации могут образовываться постоянно действующие третейские суды и третейские суды для разрешения конкретного спора (разовые).

По процессуальной компетенции суды подразделяются на суды первой инстанции, суды второй (кассационной) инстанции и суды надзорной инстанции.

Судебной инстанцией считается суд (или его структурное подразделение), выполняющий ту или иную судебную функцию, связанную с разрешением судебных дел (принятие решения по существу дела, проверка законности и обоснованности этих решений).

Суд первой инстанции — это разбирательство дела по существу с целью осуждения или оправдания подсудимого — по уголовному делу; с целью удовлетворения иска или отказа в иске — по гражданскому делу. Дела по первой инстанции могут рассматривать все суды в пределах своей компетенции, но основное количество уголовных и гражданских дел по первой инстанции рассматривают районные суды. Наиболее сложные или особого общественного значения судебные дела рассматривают по существу вышестоящие суды вплоть до Верховного Суда Российской Федерации.

Решения и приговоры большинства судов в течение установленного законом срока (7 дней для приговора, 10 дней для решения) не вступают в законную силу и могут быть обжалованы в кассационном порядке подсудимым, потерпевшим, истцом или ответчиком либо опротестованы прокурором в суд второй инстанции.

Суд второй инстанции — это суды апелляционной и кассационной инстанций. Для мировых судей и районных судов — обла-

стной и соответствующие ему суды, а для областного суда — Верховный Суд Российской Федерации. Прокуратура на основании жалоб заинтересованных лиц или кассационного протеста прокурора проверяет законность и обоснованность решений суда первой инстанции, не вступивших в законную силу.

По итогам кассационного разбирательства дела суд второй инстанции выносит определение, которое вступает в законную силу немедленно и не подлежит ни обжалованию, ни опротестованию в кассационном порядке. Оно может быть опротестовано лишь в порядке судебного надзора.

Суд надзорной инстанции по протестам лиц, указанных в законе, проверяет законность и обоснованность вступивших в законную силу решений суда первой инстанции, а также решений суда кассационной инстанции либо нижестоящей надзорной инстанции.

Судебные акты надзорных инстанций (постановления президиумов или определения коллегий) вступают в законную силу немедленно.

Подсудность дел — это распределение между судами дел, подлежащих слушанию по первой инстанции, т.е. установление конкретного суда, который должен разрешить данное дело. В судебном процессе различают два основных вида подсудности: родовую (предметную) и территориальную (местную). Родовая подсудность относит дело к ведению того или иного звена судебной системы — в зависимости от вида преступления и характера гражданского дела. Территориальная подсудность разграничивает компетенцию между судами одного и того же звена.

Верховные суды республик, краевые, областные, городские суды городов федерального значения Москвы и Санкт-Петербурга, автономной области, автономного округа в настоящее время, в частности, рассматривают и разрешают по *первой инстанции дела, связанные с нарушением законодательства о государственной тайне.*

Все гражданские дела, с точки зрения их родовой подсудности, делятся на дела подсудные по первой инстанции: мировым судьям; районным судам; верховным судам республики, областным, краевым судам, городским судам городов Москвы и Санкт-Петербурга, суду автономной области, судам автономных округов; Верховному Суду Российской Федерации.

Общее правило территориальной подсудности гражданских дел (общая территориальная подсудность) заключается в том, что иск предъявляется в суд по месту жительства ответчика. Иск к организации предъявляется по месту нахождения организации (ее имущества, а также филиала или представительства).

Альтернативная подсудность по выбору истца (заявителя) означает, что дело подсудно не только суду по месту нахождения

ответчика, но и другому суду, указанному в законе. Согласно закону, когда дело подсудно нескольким судам одного уровня, выбор суда для рассмотрения и разрешения дела принадлежит истцу (заявителю) (ст. 29 ГПК РФ).

Договорная подсудность означает, что стороны по соглашению между собой могут изменять общую и альтернативную территориальную подсудность для данного дела.

Исключительная подсудность устанавливает правила, которые исключают применение других видов территориальной подсудности, в частности, общей территориальной, альтернативной, договорной и по связи требований (дел).

В арбитражном процессе общее положение родовой (предметной) подсудности выражено в формуле: все дела, подведомственные арбитражным судам, подсудны судам субъектов Российской Федерации, за исключением дел, подсудных исключительно Высшему Арбитражному Суду РФ.

В территориальной подсудности прежде всего различают *общую территориальную подсудность*, согласно которой иски предъявляются в арбитражный суд по месту нахождения или месту жительства ответчика.

Подсудность уголовных дел характеризуют следующие признаки:

предметный (родовой) признак подсудности определяется родом (видом) преступления, составляющего предмет производства по уголовному делу, т.е. в конечном счете квалификацией преступления по статье Уголовного кодекса РФ (с помощью родового признака подсудности устанавливается, суд какого звена судебной системы компетентен рассматривать данное дело);

территориальный (местный) признак определяет подсудность уголовных дел в зависимости от места совершения преступления.

15.2. Процедура обращения в суд за судебной защитой

Для обращения в суд прежде всего необходимо определить, в какой суд обращаться, в порядке какого судопроизводства.

Основная задача гражданского судопроизводства — защита нарушенных или оспариваемых прав, свобод и охраняемых законом интересов граждан, организаций и их объединений, а также охрана государственных и общественных интересов.

В Гражданском процессуальном кодексе выделены четыре вида гражданского судопроизводства: исковое производство, приказное производство, производство по делам, вытекающим из публичных правоотношений, особое производство.

Исковое производство существует при обращении в суд за защитой нарушенных прав или интересов. По общему правилу исковое производство возникает при наличии спора. *Приказное про-*

изводство предусматривает упрощенную процедуру по выдаче судебного приказа. В *производстве по делам, возникающим из публичных правоотношений*, рассматриваются дела по жалобам на действия административных и государственных органов, общественных организаций, должностных лиц, нарушающих права и свободы граждан. *Особое производство* не связано с разрешением спора о праве, здесь нет спорящих сторон. К особому производству отнесены дела установления фактов, имеющих юридическое значение.

Возбуждение дел искового производства происходит путем подачи искового заявления. Что касается неисковых производств, то эти дела возбуждаются в суде путем подачи заявления или жалобы.

Соблюдение надлежащей формы искового заявления — важное условие соблюдения процедуры обращения в суд.

Исковое заявление подается обязательно в письменной форме и должно содержать следующие сведения:

– наименование суда, в который подается заявление;

– наименование истца, его место жительства или, если истцом является организация, ее место нахождения, а также наименование представителя и его адрес, если заявление подается представителем;

– наименование ответчика, его место жительства или, если ответчиком является организация, ее место нахождения; в чем заключается нарушение либо угроза нарушения прав, свобод или законных интересов истца и его требования;

– обстоятельства, на которых истец основывает свои требования, и доказательства, подтверждающие эти обстоятельства;

– цена иска, если он подлежит оценке, а также расчет взыскиваемых или оспариваемых денежных сумм;

– сведения о соблюдении досудебного порядка обращения к ответчику, если это установлено федеральным законом или предусмотрено договором сторон;

– перечень прилагаемых к заявлению документов.

В заявлении могут быть указаны и иные сведения, в том числе номера телефонов, факсов, адреса электронной почты, если они необходимы для правильного и своевременного рассмотрения дела.

Наряду с тем, что в исковом заявлении должны содержаться сведения, общие для всех категорий дел, имеется определенная специфика в его содержании, обусловленная целым рядом обстоятельств. Содержание искового заявления по отдельным категориям гражданских дел определяется, исходя из характера спорного материального правоотношения, субъектного состава и ряда других обстоятельств, имеющих существенное значение для правильного разрешения дела.

Важное значение имеет указание в исковом заявлении того материально-правового требования истца к ответчику, которое

составляет предмет иска. В заявлении необходимо указать, в чем заключаются нарушение или угроза нарушения прав, свобод или охраняемых законом интересов истца и его требования. Характер искового требования определяется характером спорного материального правоотношения, из которого вытекает требование истца. Просьба истца, реализованная в виде этого требования, и составляет просительный пункт искового заявления.

Цена иска, указываемая в исковом заявлении, должна быть определена в соответствии с законодательством. В исковом заявлении должна быть указана цена иска, если он подлежит оценке, а также расчет взыскиваемых денежных сумм. Кроме того, в исковом заявлении должны содержаться сведения о соблюдении досудебного порядка обращения к ответчику, когда это установлено законом или предусмотрено договором сторон.

Исковое заявление должно содержать указание на прилагаемые письменные доказательства (документы) и быть подписано истцом или его представителем при наличии у него полномочий на подписание заявления и предъявление его в суд.

К исковому заявлению должны быть обязательно приложены документы, перечень которых утвержден гражданско-процессуальным законодательством. Особо следует обратить внимание на то, что среди них должны содержаться документы, подтверждающие обстоятельства, на которых истец основывает свое требование, копии этих документов для ответчиков и третьих лиц, а также доказательство, подтверждающее выполнение обязательного досудебного порядка разрешения спора, если такой порядок предусмотрен законом или договором. Также необходимо приложить документ, подтверждающий расчет взыскиваемой или оспариваемой суммы, который должен быть подписан истцом или его представителем с приложением копий по числу ответчиков и третьих лиц.

В соответствии с законом *исковое заявление представляется в суд* вместе с копиями по числу ответчиков. Документы, прилагаемые к исковому заявлению, их перечень определяются, как правило, характером дела, подлежащего рассмотрению в суде, и зависят от того материально-правового требования, которое истец предъявляет к ответчику.

Судья принимает исковое заявление к производству суда только в том случае, если имеются для этого основания, предусмотренные законом. Принятие искового заявления может последовать только при наличии как предпосылок права на предъявление иска, так и условий, образующих порядок предъявления иска.

Отказ судьи в принятии искового заявления может последовать только по основаниям, указанным в законе, перечень которых является исчерпывающим и не подлежит расширительному толкованию.

При обращении в арбитражный суд основным процессуальным документом, без которого не может быть возбуждено дело, является *исковое заявление*, а по делам, возникающим из административных и иных публичных отношений, и по делам, рассматриваемым в порядке особого производства, — *заявление.*

Документ, исходящий от истца (*заявителя*), *должен отвечать определенным требованиям.* Требования прежде всего касаются формы и содержания заявления.

Исковое заявление подается в арбитражный суд в письменном виде и должно быть подписано истцом или его представителем.

Содержание искового заявления включает сведения, которые позволяют установить:

– какому арбитражному суду адресуется заявление;

– от кого оно исходит и к кому предъявляется иск (с подробными данными о сторонах и месте их нахождения);

– в чем заключаются исковые требования;

– какова законодательная база, на которой строятся заявленные требования;

– что входит в круг фактических обстоятельств, лежащих в основе предъявленного иска;

– какими доказательствами подтверждается существование этих обстоятельств.

В заявлении также приводится расчет взыскиваемой или оспариваемой денежной суммы, если это входит в предмет иска, указывается цена иска, если иск подлежит оценке. В случае, если федеральным законом или договором предусмотрен претензионный или иной досудебный порядок разрешения данного спора, приводятся сведения о соблюдении этого порядка.

Неотъемлемым атрибутом искового заявления является определенный состав *документов, которые прилагаются к исковому заявлению.* В перечень этих документов входят:

– уведомление о вручении или иные документы, подтверждающие направление другим лицам, участвующим в деле;

– копии искового заявления и приложенных к нему документов, которые у других лиц, участвующих в деле, отсутствуют;

– документы, подтверждающие уплату государственной пошлины в установленном порядке и размере или право на получение льгот по уплате государственной пошлины, либо ходатайство о предоставлении отсрочки, рассрочки, об уменьшении размера государственной пошлины;

– документы, подтверждающие обстоятельства, на которых истец основывает свои требования;

– копии свидетельства о государственной регистрации в качестве юридического лица или индивидуального предпринимателя;

– доверенность или иные документы, подтверждающие полномочия на подписание искового заявления;

– копии определения арбитражного суда об обеспечении имущественных интересов до предъявления иска;

– документы, подтверждающие соблюдение истцом претензионного или иного досудебного порядка, если он предусмотрен федеральным законом или договором;

– проект договора, если заявлено требование о понуждении заключить договор.

Закон предоставляет лицам, участвующим в деле, возможность направить в арбитражный суд *отзыв на исковое заявление*, в котором, в случае возражения против иска, указываются мотивы полного или частичного несогласия с требованиями истца, законодательство, а также доказательства, обосновывающие возражения. Отзыв может содержать и иные сведения, а также имеющиеся ходатайства.

Исковое заявление, подаваемое в третейский суд заинтересованным лицом, составляется в письменной форме. Оно должно содержать дату, наименование и реквизиты сторон, обоснование компетенции третейского суда, требование и обстоятельства, на которых истец основывает свое требование, подтверждающие их доказательства, цену иска (если иск подлежит оценке), перечень прилагаемых к заявлению документов и иных материалов.

Копии заявления и других приобщенных к нему документов передаются ответчику, который в срок, определенный правилами третейского разбирательства, либо до первого заседания третейского суда (если этот срок правила не содержат), вправе представить истцу и в суд отзыв на исковое заявление, изложив в нем свою позицию.

В уголовном процессе первой стадией является возбуждение уголовного дела. В уголовном законодательстве предусмотрены следующие поводы к возбуждению Уголовного дела:

– заявление о преступлении;

– явка с повинной;

– сообщение о совершенном или готовящемся преступлении, полученное из иных источников;

– наличие достаточных данных, указывающих на признаки преступления.

По результатам рассмотрения сообщения о преступлении орган дознания, дознаватель, следователь или прокурор принимает одно из следующих решений: о возбуждении уголовного дела; об отказе в возбуждении уголовного дела; о передаче сообщения по подследственности, а по уголовным делам частного обвинения — в суд.

О принятом решении сообщается заявителю. При этом ему разъясняется право и порядок обжалования данного решения.

Необходимо отметить, что расследование преступлений в сфере обеспечения информационной безопасности более сложное,

нежели других видов преступлений и требует от соответствующих должностных лиц специальной технической и юридической подготовки.

Контрольные вопросы

1. Перечислите основные разновидности судебных органов.
2. В чем заключается компетенция судов?
3. Раскройте содержание понятия «подсудность дел».
4. Раскройте основное содержание процедуры обращения в суд.

ЧАСТЬ III
ОРГАНИЗАЦИОННОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Глава 16
ОРГАНИЗАЦИОННЫЕ СИСТЕМЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

16.1. Организационные структуры государственной системы обеспечения информационной безопасности федеральных органов исполнительной власти

Наиболее развитой составляющей отечественного комплекса обеспечения информационной безопасности является *государственная система защиты информации*, в составе которой можно выделить такие *типовые организационные структуры*, как: службы контроля, надзора и обеспечения безопасности органов исполнительной власти; специализированные предприятия и организации — лицензиаты в различных областях компетенции уполномоченных органов исполнительной власти, которые являются разработчиками средств и поставщиками услуг по защите информации; сертификационно-испытательные центры; аттестационные центры; службы безопасности и защиты информации предприятий и организаций, независимо от их формы собственности.

Службы контроля и надзора органа исполнительной власти несут основную нагрузку по формированию и развитию системы защиты информации в соответствующем органе власти. Такие службы входят в состав административного аппарата органов исполнительной власти и, как правило, в их функции входят:

– разработка нормативно-методических документов отраслевого (ведомственного) уровня по выполнению требований обеспечения безопасности и защиты информации;

– разработка, организация и проведение контрольных и надзорных мероприятий в пределах установленной сферы компетентности органа государственной власти и оформление результатов проведения таких мероприятий;

– выдача предписаний об устранении нарушений требований нормативных документов;

– подготовка мотивированных предложений о полном или частичном прекращении деятельности подведомственных организа-

ций в случае, если иными мерами нарушения требований нормативных документов не могут быть устранены;

– проведение в ходе государственного контроля (надзора) разъяснительной работы по выполнению требований нормативных актов в области обеспечения безопасности и защиты информации.

Выполнение указанного перечня функций обеспечивают специалисты, соответствующие следующей *номенклатуре основных должностей*: руководитель управления, службы; руководитель отдела, сектора; специалист по направлению деятельности службы безопасности; инженер-метролог (нормоконтролер технической и организационно-распорядительной документации).

Особое место в государственной системе защиты информации занимают ***специализированные предприятия — разработчики комплексов и средств обеспечения***, а также поставщики услуг в области безопасности и защиты информации. Именно от степени их развития, уровня и качества поставляемой продукции и услуг зависит безопасность, устойчивость и надежность функционирования всей инфраструктуры информационной безопасности. Поэтому недаром одним из обязательных требований к указанным предприятиям и организациям является лицензирование их деятельности уполномоченным органом исполнительной власти в соответствии с законодательством о государственном регулировании отдельных видов деятельности.

Предлагаемые на рынке этими предприятиями *услуги организационно-технологического характера* можно классифицировать в соответствии с этапами жизненного цикла систем обеспечения информационной безопасности:

– *обследование* — услуга, которая может включать анализ защищенности используемых информационных технологий, обследование системы документооборота, обследование организации в целом (т.е. анализ влияния существующего документооборота на защищенность бизнес-процессов), проверку деятельности организации в соответствии с требованиями нормативно-правовых документов и тому подобное;

– *проектирование комплексной системы обеспечения*, при котором должен быть охвачен не только технический уровень, но и все механизмы защиты, включая организационно-правовые;

– *внедрение системы защиты информации* на договорной основе с использованием специализированных подрядных организаций, имеющих соответствующую лицензию (может дать большой эффект за счет высокой квалификации привлекаемых специалистов);

– *сопровождение систем информационной безопасности и работ по защите информации третьими лицами* (*аутсорсинг*), т.е. оказание специализированной оперативной помощи в случае внештатных ситуаций, периодическое обновление специального и обще-

системного программного обеспечения в случае появления новых атак и уязвимостей.

Организация и технологии разработки специализированных комплексов, систем и средств защиты информации принципиально не отличаются от используемых в других отраслях создания высокотехнологичной продукции, в частности средств вычислительной техники. Основная номенклатура должностей традиционна для высокотехнологичных предприятий: конструктор по наладке и испытаниям; конструктор по стандартизации; программист; технолог; электроник; техник по наладке и испытаниям.

Бурный процесс информатизации и, как следствие, все возрастающая актуальность обеспечения требований информационной безопасности приводят к необходимости видоизменения и дополнения номенклатуры специалистов. Широкое распространение общепризнанной международной практики проведения такого вида услуги, как аудит информационной безопасности, привело к появлению специалистов нового профиля — аудиторов, которые осуществляют свою деятельность в соответствии с рекомендациями *отечественных и международных стандартов*. К таким стандартам относятся:

– ГОСТ Р ИСО/МЭК 17799—2005 «Информационная технология — Практические правила управления информационной безопасностью»;

– ИСО/МЭК 17799—2000 «Информационная технология. Кодекс установившейся практики для менеджмента информационной безопасностью»;

– BS 7799 «Управление информационной безопасностью. Практические правила»;

– вторая часть BS 7799-2:2002 «Системы управления информационной безопасностью — спецификация с руководством по использованию».

Сертификационно-испытательные центры и лаборатории занимают особое место среди предприятий и организаций — лицензиатов в области обеспечения безопасности и защиты информации. Эти организационные структуры обеспечивают необходимую поддержку такой функции государственно-общественного регулирования в области информационной безопасности, как сертификацию средств и оценки качества оказания услуг по защите информации.

Наряду с лицензированием своей деятельности в области защиты информации указанные центры и лаборатории должны пройти дополнительно обязательную организационно-правовую процедуру — аккредитацию в качестве сертификационно-испытательных структур, которая в настоящее время осуществляется исключительно уполномоченными органами исполнительной власти. Реформа законодательства о техническом регулировании пока не

дает четкой правовой основы использования обязательной сертификации как механизма независимого подтверждения качества продукции и услуг в области информационной безопасности, но и не отменяет возможность применения такого механизма, по крайней мере в системе сертификации продукции, работ и услуг, средств и комплексов защиты сведений, составляющих государственную тайну. Наработанные практикой за более чем десятилетний период организационно-технологические процедуры в целом могут также с успехом применяться в системах добровольной сертификации. Поэтому существующие сертификационно-испытательные центры (лаборатории) по-прежнему будут играть ключевую роль в процессах подтверждения соответствия средств, комплексов и систем защиты установленным требованиям по безопасности информации. Номенклатура указанных должностей подобных структур также может быть дополнена новой категорией специалистов, например, «оценщик», или специалист по оценке защищенности информационных технологий, предусмотренной стандартом ГОСТ Р ИСО/МЭК 15408—2002 «Общие критерии оценки безопасности информационных технологий».

Аттестационные центры наряду с сертификацией средств, работ и услуг в области обеспечения информационной безопасности осуществляют относительно похожие процедуры подтверждения соответствия, называемые аттестацией объектов информатизации.

Как правило, по объему и характеру работ традиционные аттестационные центры (лаборатории) не имеют существенных отличительных особенностей по сравнению с сертификационно-испытательными центрами, а наиболее известные отечественные компании — поставщики услуг в области защиты информации — имеют аккредитацию по обоим видам деятельности и, соответственно, примерно одинаковую номенклатуру основных должностей.

Активно развивается также рынок образовательных услуг в области информационной безопасности по повышению квалификации специалистов, руководителей служб безопасности, руководителей IT-подразделений, пользователей средств защиты, так как необходимым условием для получения лицензии на деятельность в области защиты информации является наличие персонала необходимого уровня квалификации и подготовки. Однако система дополнительного образования в области информационной безопасности пока находится в стадии формирования, что затрудняет выделение ее типовых элементов.

Службы безопасности и защиты информации предприятий и организаций независимо от вида деятельности и форм собственности являются самой распространенной организационной структурой в рассматриваемой области общественной деятельности и по

существу составляют основу всей системы обеспечения информационной безопасности предприятий, организаций и страны в целом. Поэтому целесообразно рассмотреть вопросы их функционирования более подробно.

Непосредственная деятельность по организации функционирования и эксплуатации комплексов обеспечения информационной безопасности осуществляется штатными специалистами соответствующих структурных подразделений. Они должны иметь определенную квалификацию в соответствии с требованиями, установленными номенклатурой должностей и служащих. Типовые требования можно найти в квалификационном справочнике должностей руководителей, специалистов и других служащих, утвержденном Министерством труда и социального развития Российской Федерации в 2003 г.

16.2. Организационные структуры системы обеспечения информационной безопасности предприятия (организации)

Задачи и функции организационных структур, осуществляющих реализацию специальных защитных мероприятий (служб безопасности) на уровне предприятия (организации), определяются потребностями реальных бизнес-процессов, их спецификой и масштабами.

Традиционной задачей служб безопасности хозяйствующих субъектов является обеспечение так называемой физической защиты, под которой подразумевается охрана имущества, материальных и финансовых ценностей, а также в отдельных случаях защита персонала, прежде всего руководства, от преступных посягательств. Для решения этой задачи *служба безопасности* должна обеспечить выполнение следующих *функций*:

– организацию пропускного режима, разграничение физического доступа на защищаемые объекты;

– организацию инженерно-технической защиты охраняемых зданий и помещений объекта;

– обнаружение проникновения внешнего нарушителя на охраняемую территорию и принятие соответствующих мер противодействия;

– противодействие противоправным действиям внутренних нарушителей по отношению к имуществу и активам предприятия;

– организацию личной охраны персонала.

Менее традиционной является *задача обеспечения безопасности управления бизнес-процессами*, включающая защиту нематериальных активов и информационных ресурсов предприятия (информационная безопасность) и участие в управлении персоналом в части обеспечения лояльности и благонадежности. Реализация такой задачи *подразумевает выполнение следующих функций*:

– разведка и контрразведка, в том числе изучение криминальных аспектов рынка, организация противодействия экономическому шпионажу, сбор на законных основаниях информации о деловых партнерах и других лицах, имеющих контакты с предприятием;

– организация противодействия недобросовестной конкуренции, выявление фактов противоправного использования нематериальных активов и интеллектуальной собственности;

– организация секретного и конфиденциального делопроизводства и ведения конфиденциальных переговоров;

– обеспечение безопасности автоматизированных информационных технологий, а также информации, циркулирующей в компьютерных сетях;

– противодействие технической разведке, т.е. способам несанкционированного съема информации с помощью технических средств;

– проведение служебных расследований обстоятельств разглашения сведений, составляющих коммерческую тайну и т.д.;

– оценка лояльности и благонадежности персонала путем проведения в рамках, установленных законом, оперативно-розыскных мероприятий и выявление неблагонадежных сотрудников (группы риска) с помощью различных методов тестирования;

– подготовка персонала, в том числе нештатных сотрудников, формирование правосознания и культуры поведения всех сотрудников предприятия по вопросам обеспечения его безопасности;

– оценка эффективности работы структурных подразделений, входящих в состав службы безопасности и защиты информации.

В случае ***создания полномасштабной собственной системы безопасности и защиты информации*** наиболее эффективной является трехуровневая структура стратегического, тактического и оперативного управления.

На уровне *стратегического управления* осуществляется формулирование конкретных интересов предприятия, его бизнес-процессов и критериев обеспечения их защищенности, выделение необходимого ресурсного обеспечения. Очевидно, что решение этих задач должно быть сосредоточено на уровне высшего руководства, в структуре топ-менеджмента предприятия, где происходит утверждение соответствующей концепции развития предприятия. *Тактическое управление* осуществляет руководитель службы безопасности или должностное лицо, на которое возложены соответствующие обязанности, его заместители и руководители структурных подразделений. Основная задача тактического управления — формирование корпоративной нормативно-методической базы требований по обеспечению безопасности, их реализация и контроль за их выполнением. *Оперативное управление* включает практическую реализацию защитных функций, в том числе экс-

плуатацию специализированных технических средств и проведение организационных процедур, и осуществляется как штатными, так и нештатными сотрудниками службы безопасности, выполняющими соответствующие функции наряду с основной деятельностью.

Полномасштабный комплекс обеспечения безопасности предприятия включает следующие штатные и нештатные структуры:

– совет или комиссии по различным вопросам обеспечения безопасности, возглавляемые топ-менеджментом предприятия;

– руководство службой безопасности и руководимые им консультативно-экспертные группы;

– охранное подразделение;

– инженерно-техническое подразделение;

– аналитическую группу;

– подразделение секретного делопроизводства и ведения конфиденциальных переговоров;

– подразделение противодействия технической разведке и технической защиты информации;

– подразделение администрирования информационно-управляющих систем по требованиям безопасности информации;

– подразделение оценки лояльности и благонадежности персонала, его подготовки в области обеспечения безопасности;

– подразделение аудита систем обеспечения безопасности и оценки их эффективности.

Конкретная реализация структуры службы безопасности находится в компетенции первого руководителя предприятия. Номенклатура штатных и нештатных должностей службы безопасности на уровне предприятия может включать все перечисленные должности специализированных организационных структур. Кроме этого, в подразделениях системы управления предприятием, не связанных напрямую с обеспечением безопасности, на практике часто вводится штатная либо нештатная должность администратора информационной безопасности. Основной обязанностью такого специалиста является обеспечение защиты информационных ресурсов и администрирование соответствующих средств защиты информации на уровне конкретного подразделения.

Для ***малых предприятий с небольшими объемами бизнеса и численностью работников*** обязанности по выполнению ряда вышеперечисленных функций возлагаются на отдельных ответственных сотрудников. На предприятиях среднего масштаба создается отдельное относительно небольшое подразделение, координирующее и контролирующее выполнение функций по обеспечению безопасности другими подразделениями предприятия. Крупные фирмы и корпорации развивают службу безопасности до полномасштабной структуры, имеющей все необходимые полномочия и ресурсы для решения поставленных задач.

При этом следует иметь в виду, что *выполнение охранных функций, в том числе защиту личного состава*, в соответствии с действующим законодательством могут осуществлять либо вневедомственная охрана МВД России, либо частные охранные предприятия, действующие на основе законодательства о частной детективной и охранной деятельности. Частным охранным предприятиям разрешается оказывать различные услуги, в том числе по вооруженной охране имущественных ценностей при транспортировке и по защите жизни и здоровья персонала. Кроме этого, охранные предприятия обеспечивают проектирование, монтаж и обслуживание средств охранно-пожарной сигнализации, консалтинговые услуги по вопросам правомерной защиты от противоправных посягательств.

Другой пример *использования услуг третьих лиц по обеспечению требований информационной безопасности* характерен для предприятий и организаций негосударственных форм собственности, не имеющих собственных подразделений по защите государственной тайны. По действующему законодательству они в случае необходимости могут заключать с государственными организациями договоры об использовании их режимно-секретных органов (РСО), обеспечивающих секретное делопроизводство и режимные мероприятия в соответствии с лицензией на проведение работ с использованием сведений, составляющих государственную тайну, и на оказание услуг по защите указанных сведений.

В ходе информатизации малые и средние предприятия все чаще используют такую форму договорных услуг, как аутсорсинг информационных технологий, включая вопросы обеспечения информационной безопасности.

Одной из распространенных форм организационного обеспечения безопасности предприятия, отражающей комплексный характер рассматриваемой проблемы и один из методов ее решения, является создание отдельных комиссий. Такие нештатные структуры выполняют на временной или постоянной основе отдельные экспертные или контрольно-ревизионные функции по обеспечению безопасности, в частности инвентаризацию имущественных ценностей, нематериальных активов и информационных ресурсов, экспертизу материалов, подготовленных к публикации в средствах массовой информации, аттестацию персонала. Включение в комиссии сотрудников различных подразделений структуры управления предприятием позволяет скоординировать их взаимодействие и в целом повысить эффективность совместной деятельности.

16.3. Физическая защита

Решение задачи физической защиты предполагает проведение следующих *специальных мероприятий и действий* сотрудни-

ков службы по организации режимов обеспечения безопасности объекта:

– определение и категорирование охраняемых зон по уровню доступа;

– разработка заданий на укрепление периметров охраняемых зон (ограждение, решетки, замки и т.д.), контроль проектирования системы укрепленности периметра, прием и контроль хода эксплуатации системы;

– определение точек доступа в охраняемые зоны, разработка заданий по их оборудованию необходимыми техническими средствами, контроль проектирования и эксплуатации технических средств, разработка инструкций о порядке пропускного и внутриобъектового режимов;

– разработка заданий по применению средств охранно-пожарной сигнализации, систем видеонаблюдения, автоматизированных систем ограничения и контроля доступа в охраняемые зоны, прием и контроль эксплуатации;

– согласование порядка выноса (вноса) из охраняемых зон материальных ценностей и других видов ресурсов;

– разработка заданий, контроль проектирования, прием и контроль эксплуатации систем специальной связи, оборудования комнат и порядка приема посетителей;

– категорирование информационных ресурсов по степени секретности и конфиденциальности как нормативной основы ограничения их обращения;

– определение возможных физических каналов утечки информации с ограниченным доступом, разработка заданий на проектирование систем противодействия технической разведке, прием и контроль их эксплуатации;

– разработка порядка проведения служебных расследований по фактам нарушения пропускного и внутриобъектового режимов, а также взаимодействия с правоохранительными органами.

Указанные мероприятия позволяют обеспечить реализацию такой важной характеристики защищенности, как *конфиденциальность информации*, путем использования тех или иных технологий ограничения доступа. Однако, как правило, решение проблемы повышения эффективности бизнес-процессов требует увеличения их открытости, прозрачности как для внешней среды, так и для собственного управленческого персонала. Это позволяет в максимальной степени обеспечить масштабность производственной деятельности, ее настройку на быстро изменяющиеся условия рыночной и политической конъюнктуры. Поэтому не менее важными, а подчас и более актуальными задачами обеспечения информационной безопасности являются повышение доступности и целостности информационных активов корпорации в условиях бурного внедрения компьютерных технологий. Реализация всех ха-

рактеристик защищенности является также необходимым условием обеспечения качества бизнес-процессов за счет поддержания их непрерывности, под которой понимается и своевременное принятие управленческих решений.

Контрольные вопросы

1. Какие типовые организационные структуры входят в государственную систему защиты информации?
2. Какие функции в области обеспечения безопасности и защиты информации выполняют службы контроля и надзора органа государственной власти?
3. В чем состоит специфика государственного регулирования деятельности специализированных предприятий — разработчиков комплексов и средств обеспечения безопасности?
4. Как классифицируются услуги организационно-технологического характера в соответствии с этапами жизненного цикла систем обеспечения информационной безопасности?
5. В чем состоит специфика деятельности сертификационно-испытательных центров (лабораторий) и механизмов ее государственного регулирования?
6. Какие функции выполняет служба безопасности предприятия для решения задачи физической защиты?
7. Какие функции выполняет служба безопасности предприятия для решения задачи обеспечения информационной безопасности?
8. Как строится структура полномасштабной системы обеспечения безопасности и защиты информации?
9. Какова специфика организации и выполнения охранных функций?
10. Какие специальные мероприятия и действия должны предпринимать сотрудники службы безопасности по организации объектовых режимов?

Глава 17

КОРПОРАТИВНОЕ НОРМАТИВНОЕ РЕГУЛИРОВАНИЕ

17.1. Корпоративная нормативная база по защите информации

В силу множественности форм собственности, возможных вариантов структурного построения корпораций (предприятий, организаций, учреждений) и организации ими бизнес-процессов, корпоративные нормативные базы отличаются значительным разнообразием.

Основное назначение корпоративной нормативной базы состоит в регулировании отношений в области защиты информации, организации с учетом специфики и масштабов ее бизнес-процессов. В соответствии с общепризнанным принципом методологического и концептуального единства всех решений по защите информации нормативная база должна образовывать единую упорядоченную систему документов, построенную на так называемых типовых образцах. Под типовым образцом понимается такой документ, который отработан в соответствии с действующим законодательством, прошел достаточно широкую общественную апробацию и утвержден уполномоченными органами государственной власти. Часто в качестве аналога типовых документов используются так называемые «хорошие практики», т.е. методические рекомендации, получившие общественное признание в кругу специалистов, в том числе на мировом уровне.

В настоящее время исчерпывающий перечень типовых документов в области обеспечения информационной безопасности отсутствует, но тем не менее существует ряд практических рекомендаций по формированию структуры корпоративной нормативной базы. Одна из них состоит в том, что весь массив документов разбивается на ряд групп (сборников): нормативно-правовые акты; стандарты; корпоративные нормативные акты; методические материалы.

К этим группам сборников целесообразно также добавить массив информационно-справочной литературы.

Перечень нормативно-правовых актов и их углубленный анализ приведен в других разделах настоящего учебного пособия и в данном разделе не обсуждается.

К группе стандартов должны быть отнесены такие документы, которые содержат эталонные требования к определенным образцам продукции, работ и услуг. Стандартов достаточно много, и их

целесообразно разделить на подгруппы: концептуальные, проектирования систем защиты информации, оформления технической и организационной документации, защиты информации и контроля защищенности информации, защищенных информационных технологий. В нынешний переходный период реформирования системы технического регулирования, которая является правовой основой сертификации продукции, работ и услуг, существующие государственные стандарты (ГОСТ) постепенно теряют свою нормативную силу обязательного исполнения и к 2010 г. должны быть заменены техническими регламентами, имеющими силу закона. Стандарты, в том числе и ряд ГОСТов в области защиты информации, будут иметь рекомендательный характер как «хорошие практики», утвержденные международными организациями (международные стандарты) либо национальным органом Российской Федерации по стандартизации (национальные стандарты).

Документы корпоративного уровня, регламентирующие различные аспекты организации деятельности по защите информации, должны составлять наиболее представительную группу рассматриваемой нормативной базы. В минимальный набор таких документов входят положения о службе безопасности корпорации и ее структурных подразделениях. Типовой формат этих документов предусматривает наличие следующих разделов:

– общая часть, в которой формулируется цель создания той или иной структуры, ее основные задачи;

– источники норм или перечень нормативных актов, на основе которых организована деятельность службы и ее структурных подразделений;

– функции службы, включающие подробное изложение специальных мероприятий, которые должна осуществлять служба безопасности и ее подразделения для выполнения поставленных перед ними задач;

– структура и состав службы как организационной основы осуществления функциональной деятельности;

– номенклатура должностей, определяющая квалификационные требования к штатному и нештатному персоналу службы;

– права и обязанности руководителя службы и его подразделений, на основе которых задается правовой статус службы безопасности в общей системе управления предприятием, и меры ответственности за выполнение поставленных задач.

Следующую подгруппу нормативных документов корпорации так называемого процедурного уровня составляют *инструкции* по организации конкретных видов деятельности по обеспечению безопасности организации (специальных мероприятий), которые предусмотрены в утвержденном положении о службе безопасности. В перечень таких инструкций входят:

– порядок организации охраны предприятия;
– организация пропускного и внутриобъектового режима;
– организация эксплуатации технических средств охраны и защиты информации;
– организация секретного делопроизводства;
– порядок взаимодействия с правоохранительными органами;
– порядок применения физической силы и огнестрельного оружия;
– организация служебных расследований по фактам нарушения установленных требований безопасности;
– администрирование комплексов и средств защиты информации и т.д.

Общий объем необходимых инструкций, их содержание и структура определяются службой безопасности с учетом специфики и масштабов бизнес-процессов организации и утверждаются на уровне руководства, что позволяет применить к нарушителям установленных требований меры дисциплинарного воздействия.

Не менее актуальным в составе корпоративной нормативной базы является массив должностных инструкций конкретных работников, входящих в состав службы безопасности и его подразделений. Типовая структура должностной инструкции предусматривает наличие описания функциональных обязанностей сотрудника, его права по их выполнению, а также меры ответственности за нарушение своих обязанностей.

В группу *информационно-справочных документов* можно отнести такие материалы, которые в систематизированном виде содержат некоторую совокупность методических сведений, необходимых и достаточных для получения четкого и однозначного представления о тех или иных аспектах используемых комплексов защиты информации. В качестве основных подгрупп этой группы документов могут быть выделены словари (глоссарии), учебно-методические пособия и справочники.

Корпоративная нормативная база, как и любое другое средство защиты информации, имеет свой срок морального старения, определяющий жизненный цикл документов. При нынешних условиях бурной информатизации процессов управления организацией, широкого внедрения современных информационных технологий их срок составляет от одного до трех лет. Такой же период необходимо устанавливать и для пересмотра, переработки и переутверждения нормативных документов корпоративного уровня.

В последнее время широкое внедрение компьютерных технологий и острая потребность в обеспечении их информационной безопасности привели к появлению ряда интересных решений проблемы унификации и стандартизации в рассматриваемой сфере. Эти решения являются «хорошими практиками», утвержденными на уровне международных стандартов. В частности, предложены

унифицированные подходы по формированию нормативно-методической базы по управлению (менеджменту) комплексами обеспечения информационной безопасности на основе политики безопасности корпорации.

17.2. Политика безопасности

Существуют различные подходы к определению понятия «политика безопасности». Так, согласно стандарту ГОСТ Р ИСО/МЭК 15408—1÷3—2002 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий», более известному как «Общие критерии», *политика безопасности* — это одно или несколько правил, процедур, практических приемов или руководящих принципов в области безопасности, которыми руководствуется организация в своей деятельности.

Существуют и другие толкования этого термина:

– формальная спецификация правил и рекомендаций, на основе которых пользователи используют, накапливают и распоряжаются информационными ресурсами и технологическими ценностями;

– набор норм, правил и практических приемов, которые регулируют управление, защиту и распределение ценной информации;

– полное описание всех информационных потоков с указанием, откуда, куда, кому и какими протоколами разрешен доступ к внутренним и внешним ресурсам, а также набор организационных документов, в которых прописан регламент предоставления данных услуг, прекращения их предоставления, регламент выделения ресурсов и т.д.;

– совокупность документированных управленческих решений, направленных на защиту информационных ресурсов организации. Это позволяет обеспечить эффективное управление и поддержку политики в области информационной безопасности со стороны руководства организации.

Некоторое различие в указанных определениях подтверждает возможное многообразие подходов к практической реализации комплексов обеспечения информационной безопасности. Обобщая их, под *политикой безопасности объекта* будем понимать упорядоченную документированную совокупность управленческих и проектно-технологических решений по созданию необходимого комплекса обеспечения информационной безопасности.

Традиционные документы процедурного характера (положения, инструкции) являются нормативными предписаниями и определяют порядок организации того или иного конкретного мероприятия по защите информации. В отличие от них политика скорее

должна ответить на вопрос, что нужно сделать, чтобы в условиях ограниченных ресурсов обеспечить непрерывность бизнес-процессов за счет эффективной защиты ресурсов и активов. Именно при наличии хорошей политики безопасности можно применить продуманные (плановые, программные) методы создания соответствующего организационно-технологического комплекса. Ведь правильная постановка задачи — это уже половина успеха.

Требования к процессу создания политики безопасности должны отражать реальные потребности и не противоречить традициям и внутренней культуре организации. Это может быть достигнуто лишь при наличии видимой поддержки и одобрения со стороны руководства (собственника) организации. Поэтому основу политики безопасности, ее цели и задачи задает руководство или собственник с выделением топ-менеджера, ответственного за политику безопасности.

Оформление политики безопасности как документальной основы корпоративной нормативно-методической базы проводится поразному. Для относительно небольших предприятий с незначительным количеством сотрудников и малыми объемами бизнес-процессов политика утверждается руководством в виде единого документа, предназначенного для всех сотрудников и структурных подразделений. В противоположность этому, учитывая многоаспектный и комплексный характер проблемы, для крупных корпораций создается пакет документов, имеющих определенную иерархическую структуру. Политика безопасности верхнего уровня является общей для всех подразделений, политики второго уровня предназначаются для специализированных подразделений, например службы безопасности. На нижнем уровне находятся документы процедурного характера, отражающие частные аспекты защиты информации по организации конкретных мероприятий, в том числе должностные инструкции персонала. Отсюда вытекает важнейшее требование к хорошей политике — это практическая реализация принципа методологического и концептуального единства при решении всех вопросов защиты информации.

Политика безопасности не должна противоречить существующему законодательству в области обеспечения информационной безопасности, положениям внутренних распорядительных документов организации или контрактов, заключаемых с третьими лицами, но при этом должна соответствовать стандартам и хорошим практикам.

Политику безопасности целесообразно периодически пересматривать и обновлять, так как обеспечение информационной безопасности — это процесс, а не событие. В результате изменений условий окружающей и внутренней среды, технологий, бизнес-процессов политика безопасности должна соответственно модифицироваться, чтобы оставаться актуальной и действующей. Дол-

жны существовать правила ее пересмотра (обновления), которые бы учитывали возможность внесения необходимых изменений в политику при возникновении факторов, способных значительно повлиять на уровень информационных рисков.

Хорошей практикой является проведение независимого внешнего аудита политики безопасности для подтверждения ее эффективности и соответствия стандартам и/или требованиям других нормативных документов.

Содержание политики безопасности в наиболее распространенном подходе основывается на рекомендациях международного стандарта ISO/IEC IS 17799—2005 (second edition) (с 2007 г. — ISO/IEC IS 27002) Information Technology. Code of practice for information security management, в соответствии с которым создаваемый документ должен содержать организацию всего комплекса обеспечения информационной безопасности, включая вопросы ответственности и координации работ различных подразделений; классификацию информационных ресурсов и организацию контроля их безопасности; управление персоналом (подбор кадров, обучение, мотивация и т.д.); физическую защиту; администрирование компьютерных систем и сетей; управление доступом; разработку и эксплуатацию информационных систем; планирование непрерывности бизнес-процессов; контроль выполнения требований политики безопасности.

Такой подход наиболее целесообразен в случае разработки политики безопасности в виде одного документа. Для крупных организаций при наличии политик различного уровня для обеспечения принципа их методологического и концептуального единства первым этапом работы по созданию политики безопасности является постановка и точное формулирование целей и задач обеспечения информационной безопасности. Результатом первого этапа может быть документ общего характера под названием «Концепция обеспечения информационной безопасности». По существу концепция представляет собой политику безопасности верхнего уровня.

Концепция обеспечения информационной безопасности организации определяет систему официальных взглядов руководства (собственников) на решение проблемы обеспечения информационной безопасности и представляет собой систематизированное изложение целей и задач, основных принципов, организационных, технологических и процедурных аспектов деятельности организации в этой области на основе существующего законодательства.

Концепция должна учитывать современное состояние и ближайшие перспективы развития информационной инфраструктуры организации, существующие режимы функционирования данной системы управления, а также анализ угроз безопасности.

Основные положения и требования Концепции являются общими и распространяются на все структурные подразделения, участвующие в организации бизнес-процессов, а также на подразделения, осуществляющие сопровождение, обслуживание и обеспечение нормального функционирования информационной инфраструктуры. Основные положения Концепции могут быть распространены на договорной основе на третьих лиц, осуществляющих взаимодействие с организацией в ходе реализации бизнес-процессов.

Концепция позволяет обеспечить единую методологическую основу для формирования и проведения единой политики в области обеспечения информационной безопасности организации; принятия необходимых управленческих решений по разработке практических мер нормативно-правового, технологического и организационно-технического характера, направленных на выявление, отражение и минимизацию последствий от реализации различных видов угроз безопасности информации; координации деятельности структурных подразделений при проведении работ по созданию, развитию бизнес-процессов с соблюдением требований обеспечения информационной безопасности.

В концепции информационной безопасности должен быть обоснован выбор подхода к разработке политик безопасности нижних уровней. Один из них связан с использованием так называемых базовых показателей защищенности, представляющих набор минимально необходимых требований, выполнение которых возможно на основе типовых решений, методов и средств защиты. Лишь особо ценные бизнес-процессы потребуют и уникальных разработок, требующих дополнительных ресурсов и средств.

Концепция обеспечения информационной безопасности организации имеет примерно следующее содержание:

– общая характеристика объекта защиты (описание состава бизнес-процессов, функций и существующей технологии обработки информации);

– формулировка целей создания системы защиты, основных задач обеспечения информационной безопасности и путей достижения целей;

– основные классы угроз информационной безопасности, принимаемые во внимание при разработке подсистемы защиты;

– основные принципы и подходы к построению системы обеспечения информационной безопасности, меры, методы и средства достижения целей защиты.

Хорошей практикой считается включение в состав Концепции раздела по определению границ защищаемого объекта, так называемого «периметра защиты». Несмотря на терминологию, заимствованную из области обеспечения физической защиты объек-

тов, здесь под *периметром защиты* понимается весь спектр возможных ограничений, включая возможные внешние контакты с партнерами, вышестоящими и надзорными организациями. Политика безопасности — это руководство к действию, поэтому определение границ рассматриваемой деятельности содействует минимизации ресурсов, используемых для ее осуществления.

Важным этапом разработки политики безопасности является аудит безопасности, задачей которого является определение наиболее вероятных и наиболее опасных (с разных точек зрения) угроз, событий или действий, от которых и предстоит защищать существующие бизнес-процессы. Решение задачи состоит в изучении (обследовании) реального состояния обеспечения безопасности, а также в использовании различных методов оценки, ранжирования и категорирования опасных событий. Одним из наиболее распространенных методов является классификация угроз, оценка и анализ рисков, разработка моделей нарушителей.

Следует отметить, что аудит безопасности является мощным организационным механизмом обеспечения безопасности и должен проводиться не только на начальной стадии разработки политики безопасности. В процессе эксплуатации созданной системы защиты проведение аудита может привести и к изменению самой политики в результате модификации ранжирования угроз безопасности и необходимости принятия соответствующих мер противодействия.

Исполнители разработки политики безопасности должны находиться под контролем службы безопасности и могут являться как штатными сотрудниками, так и внешними консультантами, привлекаемыми на основе аутсорсинга.

Разработка и написание политики штатными работниками обладает рядом преимуществ, обусловленных лучшей осведомленностью о специфике системы управления и ее компонентах; более легким доступом к необходимой информации и содействие коллег; отсутствием дополнительных угроз утечки информации.

Однако такой подход имеет и недостатки, такие как субъективизм исполнителей и отсутствие специалистов нужной квалификации.

Разработка политики с использованием аутсорсинга имеет следующие преимущества: независимость экспертов; привлечение опытных и квалифицированных специалистов; наличие отработанных методик. Однако появляется проблема правильного выбора исполнителя, связанная, как правило, с высокой стоимостью работ и появлением дополнительного источника угроз.

Внедрение политики безопасности — важнейший этап во всем процессе обеспечения информационной безопасности. Очевидно, что наличие политики безопасности является необходимым, но недостаточным условием повышения уровня информацион-

ной безопасности. Созданный пакет нормативно-методических документов должен «работать». Иными словами, необходимо, чтобы его положения выполнялись своевременно и в полном объеме. Для этого следует как минимум ознакомить с ним всех ответственных сотрудников предприятия. Хорошей практикой являются также обучение и тестирование сотрудников на знание и умение выполнять требования нормативно-методических документов.

Для разработки методологии деятельности по обеспечению безопасности объекта на основе политики безопасности проводятся следующие мероприятия:

– периодическая модификация перечня угроз информационной безопасности на основе тщательного обследования всех информационных потоков системы управления бизнес-процессами, документооборота и других видов информационного взаимодействия, в том числе с внешними организациями;

– разработка методики оценки информационных рисков на основе расчета ущерба от нарушения непрерывности бизнес-процессов;

– обоснование выбора и/или модификация методов, механизмов и средств обеспечения информационной безопасности корпорации на основе критериев достаточности либо эффективность — стоимость;

– создание и модификация на основе оценки жизненного цикла корпоративной нормативно-методической базы обеспечения защиты информации;

– разработка путей и подходов к минимизации ущерба от нарушений требований по безопасности информации;

– разработка методик оценки лояльности и благонадежности персонала организации как основы минимизации угроз от утечки инсайдерской информации, мероприятий по повышению квалификации и культуры сотрудников в части обеспечения информационной безопасности.

Исходя из общих принципов построения управленческой деятельности «планирование — организация — контроль», все мероприятия и действия сотрудников службы безопасности должны строиться на основе стратегических, тактических и оперативных планов, скоординированных с планами работ других организационных структур корпорации в части обеспечения безопасности бизнес-процессов.

Естественно, «львиную» долю в деятельности службы безопасности занимают ***контрольные мероприятия и действия***, в том числе аудит информационной безопасности:

– мониторинг аномальных инцидентов в бизнес-процессах и действиях сотрудников, в том числе обнаружение вторжений в вычислительные и коммуникационные сети;

– оценка эффективности функционирования аппаратно-программных средств на основе инструкций по их использованию, организационных комплексов и действий сотрудников по выполнению утвержденных планов обеспечения защиты информации.

Контрольные вопросы

1. В чем состоит основное назначение корпоративной нормативной базы?
2. Какова структура корпоративной нормативной базы?
3. Какие разделы содержит типовой формат положений о структурных подразделениях службы безопасности?
4. Дайте перечень нормативных документов процедурного уровня.
5. Чем определяется срок жизненного цикла корпоративной нормативной базы по информационной безопасности?
6. Объясните различие в определениях политики информационной безопасности.
7. В чем состоит отличие нормативно-методических документов политики безопасности от нормативных документов процедурного уровня?
8. Какие существуют особенности документального оформления политики безопасности, и чем они объясняются?
9. Изложите типовое содержание политики безопасности, оформленной в виде единого документа.
10. В чем состоит назначение Концепции обеспечения информационной безопасности организации? Изложите общее содержание Концепции.
11. Каковы цель и задача аудита информационной безопасности?
12. Какова методология деятельности по обеспечению безопасности объекта на основе политики безопасности?
13. Дайте перечень контрольных мероприятий и действий по оценке уровня безопасности объекта.

Глава 18

ОРГАНИЗАЦИЯ ОБЪЕКТОВЫХ РЕЖИМОВ БЕЗОПАСНОСТИ

18.1. Организация пропускного режима

Обеспечение безопасности предприятия (*объекта*) предполагает использование в рамках законодательства комплекса механизмов, методов и средств, создающих необходимые ограничения доступа посторонних лиц к его ресурсам и активам. Очевидно, что эффективная реализация такой многоплановой задачи в значительной степени зависит от тщательной и кропотливой работы, которую проводят рядовые сотрудники службы безопасности по ограничению бесконтрольных действий персонала и командированных лиц на территории объекта в аспекте обеспечения его безопасности. Именно эта деятельность и обозначается понятием *особого режима объекта*, который представляет собой совокупность повседневных контрольно-учетных мероприятий по обеспечению выполнения требований его безопасности.

Практика обеспечения безопасности так называемых режимных объектов показала, что всю совокупность *специальных контрольно-учетных мероприятий* по функциональному назначению условно можно разделить на следующие *виды*: *пропускной режим*, основной целью которого является организация физической защиты внешнего периметра объекта и соответствующего санкционированного допуска сотрудников и других лиц для выполнения своих служебных обязанностей; *внутриобъектовый режим*, обеспечивающий выполнение требований безопасности на территории и в служебных помещениях режимного объекта и направленный, как правило, на противодействие внутренним угрозам.

Пропускной режим — это совокупность правил, регламентирующих порядок входа (выхода) физических лиц, въезда (выезда) транспортных средств на режимный объект, вноса (выноса), ввоза (вывоза) документов и вещей, а также совокупность мероприятий по реализации этих правил.

Пропускной режим вводится для исключения проникновения посторонних лиц на территорию режимного объекта, в его административные и производственные здания, а также в охраняемые по требованиям режима секретности зоны (категорированные помещения), для ограничения посещения должностными лицами режимных помещений без служебной необходимости, запреще-

ния вноса (ввоза) на территорию объекта посторонних предметов и технических средств, выноса (вывоза) материальных ценностей, документов и других нематериальных активов без разрешения уполномоченного должностного лица.

Пропускной режим предусматривает, в частности, оборудование и организацию работы контрольно-пропускных пунктов (постов). С этой целью ответственные работники службы безопасности должны проанализировать организационную структуру предприятия, места расположения и архитектуру его отдельных производственных и служебных помещений, характер производственной деятельности (производства) в них.

Выяснение этих вопросов позволяет: выделить объекты и территории предприятия, на которых необходимо организовать охранный пропускной режим; определить характер контрольно-пропускных пунктов (КПП) для пропуска физических лиц и транспортных средств, вывоза (ввоза) материальных ценностей; определить перечень предметов, запрещенных к проносу (провозу) в охраняемые зоны режимного объекта.

На основе прогноза объема потоков физических лиц, транспортных средств, грузов, материальных ценностей, пересекающих охраняемый периметр предприятия, задается необходимая пропускная способность КПП и возможный вариант оптимизации автоматизированного контроля «прохода», «проезда», «проноса» и «провоза» на границах охраняемых объектов и территорий.

Организация пропускного режима предполагает также разработку определенного нормативного обеспечения этой деятельности, согласованного с общей нормативно-правовой базой предприятия. Важность этого момента определяется тем, что вводимые требования по ограничению доступа должны строго соответствовать действующему законодательству и ни в коей мере не противоречить конституционным правам и свободам.

Пропускной режим осуществляется на основании внутреннего нормативного документа — *инструкции*, утверждаемой руководителем предприятия.

Инструкция, как правило, начинается с описания общих целей и задач, решаемых системой пропускного режима; предусматривает создание специального структурного подразделения (бюро пропусков) по оформлению документов, дающих право на проход; вводит систему пропусков для физических лиц и транспортных средств, задает ответственность должностных лиц, в обязанности которых входит организация этого режима; определяет соответствующие структурные подразделения, осуществляющие его практическую реализацию.

Основным разделом инструкции служит ***порядок пропуска (прохода) физических лиц, вывоза (ввоза) на территорию объекта***, который определяет:

– основания права на проход, которыми являются удостоверения сотрудников (работников) предприятия, временные и разовые пропуска, магнитные карты (для электронных проходных), пропуска-вкладыши к удостоверению личности (паспорту);

– перечень сторонних организаций, контрольно-надзорных органов государственной власти, имеющих право прохода по своим служебным удостоверениям;

– порядок предъявления документов на проход, как правило, в развернутом виде в руки дежурному службы охраны для однозначной идентификации при каждом входе (выходе) на охраняемый объект;

– правила выдачи и оформления временных и разовых пропусков;

– правила досмотра с согласия сотрудника его личных вещей (портфелей) при наличии оснований для подозрений о возможности вноса (выноса) запрещенных предметов, при отказе от досмотра предусматриваются места временного хранения таких вещей;

– предельные сроки пребывания работников на своих рабочих местах и правила оформления разрешения на сверхурочные работы;

– порядок прохода делегаций, иностранных граждан, который, как правило, осуществляется по списку в сопровождении ответственного должностного лица.

Одним из разделов инструкции определяются ***правила проезда (выезда) транспортных средств***, которые предусматривают:

– основания для въезда (выезда) служебного транспорта в виде пропусков установленного образца и/или служебных удостоверений водителей и пассажиров;

– перечень должностных лиц, имеющих право въезда на объект на служебном автотранспорте без проверки документов;

– правила пропуска автотранспорта сторонних организаций по разовым пропускам на въезд автотранспорта в сопровождении сотрудника подразделения, принимающего посетителей или груз, водитель и пассажиры пропускаются на объект в соответствии с установленным порядком для физических лиц;

– порядок въезда автотранспорта для ликвидации чрезвычайных ситуаций, осуществляемый по личному распоряжению уполномоченного должностного лица, в ведении которого находится режимный объект;

– основания для ввоза грузов на режимные объекты, которыми являются товаротранспортные накладные и подтверждение ожидаемого груза от руководителей заинтересованных подразделений;

– основания для вывоза грузов (материальных ценностей) в виде материального пропуска, для выдачи которого оформляется по установленной форме заявка, подписанная материально-ответственным лицом и уполномоченным должностным лицом;

– обязанность дежурного службы охраны по проверке соответствия вывозимого груза (материальных ценностей), указанных в материальном пропуске.

В заключение инструкция определяет ***порядок и правила контроля пропускного режима***. Контроль за несением службы по организации охраны периметра, действий оперативных дежурных, а также наряда охраны осуществляется уполномоченными должностными лицами, назначенными руководителем предприятия.

Эффективность пропускного режима во многом определяется тем, как организована охрана объекта. В соответствии с действующим законодательством выполнение охранных функций могут осуществлять только специализированные силы и организации. Например, охрана так называемых критических объектов крупных организаций и предприятий (атомные электростанции, химические производства и т.д.) осуществляется внутренними войсками или подразделениями вневедомственной охраны МВД России. Действующее законодательство разрешает указанным структурам обеспечивать охрану имущества на договорной и внедоговорной основе. Кроме этого, им разрешены контроль деятельности, используемой на предприятиях других охранных структур, испытание систем и технических средств охранной сигнализации, осуществление технического надзора за оборудованием объектов средствами охранной сигнализации. В ряде случаев охрану государственных объектов осуществляет ведомственная охрана, создаваемая отдельными федеральными органами исполнительной власти. Их перечень устанавливает Правительство Российской Федерации. Действующее законодательство разрешает привлечение ведомственной охраны на договорной основе для защиты имущества предприятий, отличных от государственной формы собственности.

Основные задачи ведомственной охраны: защита охраняемых объектов от противоправных посягательств; обеспечение на охраняемых объектах пропускного режима; предупреждение и пресечение преступлений и административных правонарушений на охраняемых объектах.

Выполнение охранных функций, в том числе защиты личного состава на малых и средних предприятиях, как правило, осуществляют частные охранные предприятия (ЧОП), действующие на основе законодательства о частной детективной и охранной деятельности. Частным охранным предприятиям разрешается оказывать различные услуги, в том числе по вооруженной охране имущественных ценностей при транспортировке и защите жизни и здоровья персонала. Кроме этого, ЧОП могут обеспечивать проектирование, монтаж и обслуживание средств охранно-пожарной сигнализации, консалтинговые услуги по вопросам правомерной защиты от противоправных посягательств.

Нормативной основой организации охранных мероприятий является соответствующая инструкция, утверждаемая руководителем предприятия. Она должна включать общие положения несения охранной службы, состав суточного наряда, его оснащение, особые обязанности должностных лиц охранных нарядов, действия охраны при объявлении тревоги, при пожаре и других видах чрезвычайных ситуаций.

Общее руководство организацией и несением службы нарядами охраны, а также взаимодействие с соответствующими правоохранительными органами и другими охранными структурами, как правило, осуществляет руководитель ЧОП, предоставляющий на договорной основе соответствующие охранные услуги.

Личный состав нарядов охраны непосредственно подчиняется руководителю ЧОП и дежурному по объекту. В нерабочее время и в отсутствие руководителя охранного предприятия руководство охранной службой осуществляет дежурный по объекту.

Перевозка и сопровождение специальных грузов, порядок приема и сдачи под охрану режимных помещений, а также ведение личной охраны регламентируются отдельными инструкциями.

Тревога объявляется при нападении на охраняемый объект или караульный пост. Сигнал тревоги может быть подан сотрудником охраны с поста или поступить на пульт охранной сигнализации. Сигналами тревоги могут являться указания уполномоченного должностного лица, звуковой и световой сигналы, окрики «тревога» и т.д.

Дежурный по объекту при получении тревожных сигналов в зависимости от складывающейся обстановки направляет на место происшествия группу быстрого реагирования из резерва охраны, усиливает охрану на постах объекта, выясняет обстоятельства тревоги, определяет необходимость дополнительных средств охраны и ликвидации причин тревоги и докладывает о принятых мерах руководству охраны и предприятия.

Сотрудники охраны, несущие службу на пропускных постах, при объявлении тревоги прекращают допуск (вход) на объект и выход с объекта всех лиц, за исключением руководителей объекта, которым они подчиняются по службе.

Сотрудники охраны, находящиеся в резерве, по указанию дежурного по объекту экипируются с учетом характера тревоги и следуют на место происшествия, усиливают посты, а также выполняют другие указания руководства охраны.

При пожаре и возникновении других чрезвычайных ситуаций дежурный по объекту при получении соответствующей информации объявляет тревогу.

Уполномоченные должностные лица в пределах своих полномочий руководят действиями личного состава предприятия в соответствии со сложившейся обстановкой, привлекая при необхо-

димости технических специалистов и персонал ЧОП, о чем немедленно докладывают руководству. Вызывается служба экстренного вызова, аварийные бригады соответствующих коммунальных служб, обеспечивается встреча специалистов и их допуск на объект в сопровождении службы охраны. При принятии решения об эвакуации персонала объекта и посетителей, а также материальных ценностей создаются временные посты для их охраны и усиления пропускного режима.

18.2. Организация внутриобъектового режима

Внутриобъектовый режим обеспечивает выполнение требований безопасности на территории и в служебных помещениях режимного объекта и направлен, как правило, на противодействие внутренним угрозам.

К ***организационному обеспечению внутриобъектового режима традиционно относят*** мероприятия по обеспечению охраны выделенных помещений, категорированных по специальным требованиям безопасности. Так, посещение посетителями данных помещений ограничивается организационно-техническими мерами. После окончания работы в них все двери, окна и форточки должны быть надежно заперты, поставлены на охранную сигнализацию и опечатаны. Все ключи от дверей охранных зон должны быть сданы на охранный пост с отметкой в специальном журнале, с подписью лиц, сдавших и принявших ключи. Отключение охранной сигнализации и выдачу ключей для вскрытия помещений осуществляет дежурный охраны поста по требованию лиц, имеющих на это право, на основании списка и подписи сотрудников в специальном журнале. Все сотрудники, имеющие санкционированный доступ в охранные зоны, должны знать способы извещения оперативно-дежурных служб. В охранных зонах запрещается фото-, кино-, видеосъемка, а также пользование мобильными телефонами и портативными ЭВМ.

Более опасным внутренним угрозам должен соответствовать и больший объем деятельности по организации внутриобъектового режима, к которой целесообразно отнести режим секретности и конфиденциального делопроизводства; режим противодействия утечки информации по техническим каналам.

Иногда, учитывая важность и значительный объем мероприятий по организации указанных режимов, их выделяют в самостоятельные направления деятельности службы безопасности, хотя по существу это также отдельные составляющие внутриобъектового режима.

Режим секретности и конфиденциального делопроизводства устанавливается в соответствии с нормами информационного права, согласно которым государственные информационные ресур-

сы, а по умолчанию и ресурсы коммерческих структур, могут иметь: различные правовые режимы открытые (общедоступные) и с ограниченным доступом, охраняемые в режиме некоторой тайны.

В зависимости от вида тайны режим ограничения доступа к информационным ресурсам с организационно-правовой точки зрения имеет существенные различия.

Так, для сведений, составляющих государственную тайну, законодательно устанавливается единый порядок их выделения, использования и обращения. В соответствии с законодательством в области защиты государственной тайны уполномоченными органами исполнительной власти вводятся очень жесткие обязательные нормы государственного регулирования практически всех организационных процедур. Их нарушение влечет за собой определенную юридическую ответственность.

Для других видов сведений конфиденциального характера законодательные нормы, как правило, имеют декларативный характер. Незначительное количество прописанных в законах норм можно рассматривать лишь как рекомендации обладателю информации, который вправе сам принимать решения о ее защите. В связи с этим он сам принимает на себя весь риск, связанный с реализацией угроз информационной безопасности. Хотя в нынешнем уголовном кодексе существует статья, в соответствии с которой можно понести наказание за разглашение банковской или коммерческой тайны, судебная практика весьма ограничена. Поэтому ответственность, как правило, ограничивается мерами дисциплинарного воздействия и лишь в редких случаях — гражданской ответственностью.

Практика защиты несекретных сведений служебного характера имеет несколько другой характер. После принятия в 1993 г. Закона Российской Федерации «О государственной тайне» Правительством Российской Федерации было принято постановление от 13 ноября 1994 г. № 1233, которое ввело в действие «Положение о порядке обращения служебной информации ограниченного распространения в федеральных органах исполнительной власти». Согласно этому нормативному правовому акту, «к служебной информации ограниченного распространения относится несекретная информация, касающаяся деятельности организаций, ограничение на распространение которой диктуется служебной необходимостью». Указанный нормативный акт заложил правовую основу для широкого распространения на практике простых и хорошо известных организационных процедур делопроизводства и обращения документов с грифом «Для служебного пользования». В частности, такой порядок принят в банковской системе Российской Федерации.

Совет директоров Банка России утвердил аналогичное положение для подведомственных организаций, причем в отличие от

правительственного акта к сведениям ограниченного распространения отнесены банковская, коммерческая и служебная тайны.

Рассматривая различные правовые режимы информации, следует отметить, что отнесение тех или иных сведений к категории открытой (общедоступной) информации не означает наличия права их бесконтрольного использования. Речь идет, прежде всего, о так называемой интеллектуальной собственности, к которой, в частности, относятся программы для ЭВМ и базы данных, имеющих правовой статус объектов авторского права. Если такие объекты создаются в рамках выполнения служебного задания, то имущественные права на них принадлежат работодателю и, соответственно, эти объекты также должны быть включены в перечень защищаемых активов.

Режим секретности устанавливает единый порядок обращения со сведениями, составляющими государственную тайну, и предназначен прежде всего для противодействия утечке секретной информации по агентурным каналам, т.е. угрозам от внутренних нарушителей.

Организация режима секретности включает проведение следующих процедур:

– засекречивание (рассекречивание) путем установления степени секретности сведений, содержащихся в документах, используемых или создаваемых на режимном объекте;

– оформление допуска, т.е. особых видов документов, подтверждающих наличие у сотрудника санкции на работу с документами, содержащими государственную тайну;

– контроль выполнения должностными лицами установленных правил работы с секретными документами;

– ведение секретного делопроизводства.

Засекречивание сведений инициируется исполнителем документа на основании действующего на предприятии и утвержденного его руководителем перечня сведений, составляющих государственную тайну. Разработку такого перечня осуществляют сотрудники режимно-секретных органов (РСО), структурно входящие в службу безопасности на основании отраслевых или ведомственных перечней, утвержденных уполномоченным руководителем органа государственной власти, применительно к специфике своего предприятия.

Проект перечня рассматривается специально создаваемой из числа ведущих специалистов предприятия экспертной комиссией, после заключения которой перечень утверждается руководителем предприятия.

Сведения, включенные в перечень, должны быть сгруппированы по степени их секретности. В соответствии с правилами, утвержденными Правительством Российской Федерации 4 сентября 1995 г., к сведениям особой важности относят сведения,

распространение которых может нанести ущерб в одной или нескольких областях деятельности, указанных в законе о государственной тайне. К совершенно секретным относятся сведения, разглашение которых связано с ущербом на уровне федерального органа исполнительной власти или отрасли экономики, к секретным — на уровне предприятия, учреждения и организации.

Перечень должен пересматриваться по мере изменения существенных условий деятельности предприятия, но не реже, чем через пять лет. Для рассекречивания или проверки обоснованности также используется механизм комиссионной экспертной оценки, проводимой с участием работников РСО, с обязательным утверждением результатов руководителем предприятия.

Допуск работников к сведениям, составляющим государственную тайну, означает формальное санкционирование возможности работы с такими сведениями, в то время как доступ — это санкционированное полномочным должностным лицом ознакомление с конкретными сведениями. Организационные процедуры оформления допуска регламентируются соответствующей инструкцией, утвержденной Постановлением Правительства Российской Федерации от 28 октября 1995 г. № 1050. Начальным этапом этого процесса является разработка сроком на 5 лет номенклатуры должностей предприятия, подлежащих оформлению на допуск к сведениям, составляющим государственную тайну. Такая номенклатура является необходимым документом для последующего согласования и взаимодействия с уполномоченным органом государственной власти, осуществляющим проверочные мероприятия. Наименование должностей должно соответствовать конкретно выполняемой работе с использованием государственной тайны с учетом степени секретности используемых сведений. Каждой степени секретности соответствует своя форма допуска: первая — особой важности, вторая — совершенно секретно, третья — секретно. Это означает, что работник с первой формой допуска может быть допущен ко всем сведениям, составляющим государственную тайну; наличие второй формы дает возможность работы с совершенно секретными и секретными сведениями; наличие третьей — только с секретными.

Очевидно, что каждой форме допуска соответствуют различные объем и уровень проверочных мероприятий. Если в случае допуска по первой и второй форме проверка осуществляется уполномоченным органом государственной власти, то для третьей формы допуск оформляется РСО самого предприятия, за исключением руководителей, работников специальных объектов и лиц, имеющих двойное гражданство.

Участие самого работника в процедуре оформления допуска заключается в правильном и достоверном заполнении анкеты и подписании договора об оформлении допуска к государственной

тайне. В договор, наряду с типовыми условиями, рекомендуется включать особые пункты, например конкретные сроки ограничения выезда за границу, порядок хранения заграничного паспорта и т.д.

При снижении степени секретности используемых работником сведений форма допуска может быть понижена на основании решения руководителя предприятия с возможностью ее восстановления без дополнительных проверочных мероприятий.

Основной контроль и учет деятельности сотрудника с использованием сведений, составляющих государственную тайну, проводится путем оформления доступа. Данные процедуры включают получение письменной санкции уполномоченного должностного лица на использование строго дозированного объема таких сведений, выдачу документов под расписку, занесение факта использования конкретных сведений в учетную карточку. Оформление доступа лицам, прибывшим в служебную командировку, производится лишь при наличии удостоверения личности, предписания на выполнение соответствующего задания и справки о наличии допуска.

При обращении секретных документов РСО обеспечивают периодический контроль выполнения должностными лицами следующих правил:

– любая передача секретных документов сопровождается собственноручной подписью участников процедуры с регистрацией в учетных формах РСО;

– работа с секретными документами может осуществляться только в специально аттестованных по требованиям безопасности информации служебных помещениях;

– при работе с секретными документами на рабочем месте должен находиться минимально требуемый объем сведений, составляющих государственную тайну;

– хранение секретных документов производится в специально оборудованных хранилищах (библиотеках) РСО, в сейфах с обеспечением минимально возможного риска их утраты за счет пожаров, протечек и т.д.

– выдача секретных документов на руки исполнителям производится на период не более одного рабочего дня, при временном выходе из рабочего помещения исполнитель обязан убрать секретный документ в свой личный сейф;

– запрещается хранение секретных документов в рабочих столах вместе с несекретными материалами;

– при приеме посетителей секретные документы должны находиться в положении, неудобном для обозрения;

– категорически запрещается вынос секретных документов за пределы охраняемого периметра режимного объекта;

– при окончании работы с секретными документами необходимо проверить их и сдать в библиотеку РСО.

Секретное делопроизводство задает организационные механизмы, правила и процедуры работы с государственной тайной. Документы, содержащие секретные сведения, могут разрабатываться только в специальных блокнотах и рабочих тетрадях, подлежащих учету, регистрации и хранению в библиотеках РСО. Создается минимально возможное количество копий секретного документа, определяемое исключительно служебной необходимостью. Разрабатываемый документ должен содержать минимально возможный объем секретных сведений, необходимых для понимания сути его содержания. Для копирования секретных документов предусматривается специальная разрешительная процедура его осуществления исключительно через РСО. Документирование, т.е. оформление по нормативно установленным правилам, осуществляют сотрудники РСО с обязательным указанием грифа секретности, номера каждого экземпляра, места разработки, исполнителей, количества листов экземпляров и датой документирования.

Передача секретных документов третьим лицам производится исключительно РСО предприятия. Полностью оформленный документ перед отправкой помещается в специальную упаковку (пакет), исключающую несанкционированный доступ. Пересылка секретных документов в другие города осуществляется службами специальной почтовой связи; в рамках одного города используют собственных курьеров, которых обеспечивают служебным транспортом и охраной.

Учет передачи документов осуществляется путем регистрации в разносных книгах, по распискам, реестрам под собственноручную подпись ответственного сотрудника РСО принимающей стороны, которая скрепляется печатью с проставлением времени и числа. Как и каждый документ, секретные сведения имеют свой жизненный цикл, по окончании которого их материальные носители подлежат физическому уничтожению. Для проведения этой процедуры приказом руководителя предприятия назначается комиссия в составе не менее трех человек. Комиссия уточняет необходимость и обоснованность уничтожения, проводит сверку уничтожаемых носителей по журналам и карточкам учета, составляет соответствующий акт, который представляется на утверждение руководителю предприятия и передается на учет и хранение в РСО.

В соответствии с законодательством режим защиты конфиденциальных сведений определяется собственником (владельцем, обладателем) информационного ресурса. Поэтому задача организации по созданию и обращению несекретных документов конфиденциального характера не имеет общепринятых типовых решений. В частности, широко распространены рекомендации по защите коммерческой тайны, которые предусматривают процедуры, аналогичные установленным для секретного делопроизводства. В то же время в практической деятельности наиболее часто

используется режим делопроизводства и обращения документов с грифом «Для служебного пользования» (ДСП). Как правило, этот режим предусматривает:

– отнесение сведений к категории ограниченного распространения, он определяется исполнителем и утверждается должностным лицом, подписывающим соответствующий документ (пометка «ДСП» и номер экземпляра проставляются в правом верхнем углу первой страницы документа, на обложке и титульном листе издания, а также на сопроводительном письме к такому документу);

– прием и учет (регистрация) документов осуществляется канцеляриями, ведущими прием и учет несекретной документации;

– при создании документа с грифом «ДСП» на обороте последнего листа указывается количество распечатанных экземпляров, исполнители и дата оформления (оформленные документы вместе с черновиками и вариантами проекта передаются в службу регистрации для регистрации и уничтожения черновиков с отражением этого факта в учетных формах);

– отдельный учет от несекретной документации;

– осуществление передачи с разрешения руководителя исключительно под расписку, а пересылку — заказными или ценными почтовыми отправлениями;

– размножение — только с разрешения уполномоченного должностного лица с поэкземплярным учетом;

– хранение в надежно запираемых и опечатываемых шкафах;

– группировку исполненных документов в дела, соответствующие номенклатуре дел несекретного делопроизводства, с проставлением на обложке дела грифа «ДСП»;

– комиссионную проверку наличия документов, которая проводится не реже одного раза в год.

В настоящий период становления информационного общества технологии бумажного делопроизводства и соответствующие средства их защиты постепенно теряют свою актуальность в связи с переходом к автоматизированной поддержке основных процессов управленческой деятельности, в том числе делопроизводства и документооборота. Стремительный рост количества и качества программных средств, предназначенных для поддержки документооборота, привел к появлению отдельного сегмента мирового рынка информационных технологий, для обозначения которого используется англоязычный термин — «Electronic Document Management System» (EDMS). В настоящее время нет общепринятого варианта перевода этого понятия на русский язык. Самыми распространенными вариантами являются такие, как «системы электронного управления документами», «системы управления электронным документооборотом», «системы управления электронными документами» и т.д. Точку в этой дискуссии должны

поставить законодатели при принятии законов «Об электронном документе» или «Об электронном документообороте». Мы же пока будем использовать оригинальную англоязычную версию сокращения — EDMS.

На первом этапе развития подобных систем основной предпосылкой их стремительного роста являлись преимущества, связанные с простой заменой бумажных носителей информации на электронные. Однако к настоящему времени актуальность EDMS стала определяться общими тенденциями развития общественной деятельности, которые наиболее ярко проявляются на примере организации современной экономики. Решающим условием успешного бизнеса является фактор времени, необходимого для принятия управленческого решения и его документального оформления. Поэтому развитие EDMS идет по пути интеграции технологий делопроизводства и документооборота с системами поддержки коллективного принятия управленческих решений и контроля над исполнением их решения.

Решающим условием успешного развития EDMS стало понимание того, что высокая степень автоматизации управленческой деятельности связана с резким повышением рисков и угроз безопасности. Наряду с традиционной проблемой обеспечения конфиденциальности, при стремительном усложнении программно-аппаратных комплексов все большую значимость приобретают вопросы повышения доступности, а также защиты от нарушений физической и логической целостности EDMS и используемых информационных ресурсов. Поэтому обеспечение высокого уровня надежности и безопасности в целом является приоритетной задачей при построении EDMS. Иными словами, вопросы обеспечения конфиденциальности решаются как бы «автоматически» (по умолчанию) и входят в общие процедуры обеспечения безопасности организационно-технологического характера, главной из которых является обеспечение эффективного контроля доступа к информационным активам предприятия.

Современные EDMS обеспечивают процесс создания, управления доступом и распространения больших объемов документов в компьютерных сетях, а также контроль над потоками документов в организации. Документы хранятся в специальных хранилищах или в иерархии файловой системы. Типы файлов, которые, как правило, поддерживают системы EDMS, включают не только текстовые документы, но и их образы, электронные таблицы, аудио-, видеоданные. К общим возможностям данных систем относятся также управление доступом и обеспечение других факторов безопасности информации.

Ниже приведены основные функциональные возможности EDMS, которые используются в том числе для обеспечения требований конфиденциальности бизнес-процессов:

– поддержка эффективного накопления, управления и доступа к информации и знаниям, что позволяет одновременно обеспечить вопросы управления персоналом за счет определенной формализации деятельности каждого сотрудника и анализа всей предыстории его деятельности;

– протоколирование деятельности предприятия в целом, автоматизированный анализ деятельности подразделений и каждого отдельного сотрудника, что облегчает проведение внутренних служебных расследований и выявление «узких мест» в их работе;

– оптимизация бизнес-процессов и автоматизация механизма контроля их выполнения;

– минимизация бумажного документооборота в управленческих процедурах предприятия, что дает экономию ресурсов за счет сокращения издержек на управление, в том числе контроля информационных потоков;

– существенное увеличение сохранности и безопасности хранения документов в электронных архивах.

Современные подходы к созданию EDMS можно продемонстрировать на примере технологии workflow, которая является основой наиболее конкурентоспособных систем на рынке информационных технологий. Стандартизацией и продвижением этой технологии занимается международная организация WfMC (Workflow Management Coalition) (http://www.wfmc.org).

Термин «workflow» также пока не имеет подходящего аналога в русском языке. Его буквальный перевод означает поток работ, или рабочий поток, в то время как в литературе используются термины «деловой процесс» или «бизнес-процесс». Однако реальное содержание понятия workflow более глубокое.

Согласно глоссарию WfMC, бизнес-процесс — это одна или более связанных между собой процедур или операций (функций), которые совместно реализуют некую бизнес-задачу или политическую цель предприятия, как правило, в рамках организационной структуры описывающей функциональные роли и отношения. Бизнес-процесс объединяет поток работ и функции, которые должны выполняться над элементами (заданиями) этого потока, персонал и оборудование, которые реализуют эти функции, а также правила, управляющие последовательностью их выполнения. Назначение технологии workflow — это автоматизация таких процедур в контексте управления ими.

Принципиальные особенности рассматриваемой технологии вытекают из определений, данных в глоссарии WfMC: Workflow — автоматизация, полностью или частично, бизнес-процесса, при которой документы, информация или задания передаются для выполнения необходимых действий от одного участника к другому в соответствии с определенным набором процедурных правил.

Система управления workflow — система, которая описывает поток работ (по сути, бизнес-процесс), создает его и управляет им при помощи программного обеспечения, которое способно интерпретировать описание процесса, взаимодействовать с участниками потока работ и при необходимости вызывать соответствующие программные приложения и инструментальные средства.

Таким образом, подходы на основе workflow означают автоматизацию процессов, а не отдельных функций исполнителей. Такие подходы отражают постепенный переход управленческой деятельности на новые принципы: от функционально-ориентированной модели в направлении процессной ориентации. В первой модели последовательность действий сотрудников и правила их взаимодействия определены должностными инструкциями, а контроль их выполнения осуществляет, как правило, руководство.

Процессный подход концентрирует внимание именно на правилах и взаимодействиях участников процесса и позволяет значительно снизить риски информационных угроз, причиной которых являются размытость и неопределенность процедур взаимодействия. С позиций интересов предприятия «промышленные» методы руководства и управления на основе workflow, усиливая контроль над производительностью и качеством выполнения задач, одновременно повышают конфиденциальность за счет ужесточения контроля доступа к информационным ресурсам. Интересы клиента защищаются за счет улучшения качества обслуживания, повышения его оперативности, упрощения доступа и предоставления более полной и четкой информации. Не забыты и исполнители, каждый из которых не только имеет наглядное представление перечня своих функций, но и контекст каждой функции в аспекте организации работы. Это обеспечивает быстроту и качество исполнения при высокой степени комфорта. С точки зрения организации контрольно-надзорных процедур workflow дает в распоряжение организационных аналитиков всю необходимую статистику для анализа рабочих нагрузок, затрат, периодов пиковой нагрузки, нештатных ситуаций и других аспектов, необходимых для обеспечения безопасности предприятия. На основе таких технологий как workflow может быть создан реальный, а не умозрительный комплекс организационно-технического обеспечения информационной безопасности.

Одной из важнейших функций внутриобъектового режима является ***противодействие технической разведке***. Под ней понимается комплекс мероприятий организационно-технического характера, проводимых с целью исключения или существенного затруднения получения данных о режимном объекте по техническим каналам утечки информации. В практике защиты коммерческих секретов этот вид деятельности получил название «защита от промышленного шпионажа».

Данное направление деятельности среди различных аспектов защиты информации имеет важное самостоятельное значение, особенно в случае защиты сведений, составляющих государственную тайну. Перечень одних только видов технической разведки насчитывает более 20, начиная от космического наблюдения до снятия акустической информации с каналов связи общего пользования. И, как правило, эффективное противодействие также осуществляется техническими методами и средствами. Главной организационной составляющей этого направления для обеспечения внутриобъектового режима является создание такой структуры, как постоянно действующая техническая комиссия (ПДТК), в состав которой, кроме ответственных работников РСО, включаются также квалифицированные и компетентные технические специалисты предприятия.

ПДТК является консультативным органом при руководителе предприятия по вопросам режима секретности и противодействия техническим разведкам.

К *основным функциям и задачам ПДТК* относятся:

– выявление возможных технических каналов утечки информации, присущих данному предприятию;

– планирование и координация всех внутренних мероприятий по обеспечению режима секретности и противодействию технической разведке;

– экспертиза проектов по разработке и результатам реализации мероприятий по своевременному закрытию выявленных каналов утечки информации с ограниченным доступом;

– организация и ведение общей профилактической работы по защите информации ограниченного доступа от технических разведок.

Минимально возможный объем таких мероприятий сводится к выделению и оборудованию техническими средствами противодействия специальных помещений (охранных зон) и разработки соответствующих правил их эксплуатации.

Хорошей практикой, использование которой в государственной системе защиты информации является обязательной, служит аттестация объектов информатизации по требованиям безопасности информации. Организацию этой деятельности осуществляет Федеральная служба по техническому и экспертному контролю (ФСТЭК России) как правопреемник Государственной технической комиссии при Президенте Российской Федерации.

Под ***аттестацией объектов информатизации*** понимается комплекс организационно-технических мероприятий, в результате которых посредством специального документа «Аттестат соответствия» подтверждается, что объект соответствует требованиям стандартов или иных нормативно-технических документов по безопасности информации, утвержденных уполномоченными органа-

ми государственной власти. Наличие на объекте информатизации действующего «Аттестата соответствия» дает право обработки информации с установленным уровнем секретности (конфиденциальности) и на период времени, определенным в «Аттестате соответствия».

Обязательной аттестации подлежат объекты информатизации, предназначенные для обработки информации, составляющей государственную тайну, для управления экологически опасными объектами, для ведения секретных переговоров. В остальных случаях аттестация носит добровольный характер (добровольная аттестация) и может осуществляться по инициативе заказчика или владельца объекта информатизации. Аттестация по требованиям безопасности информации предшествует началу обработки подлежащей защите информации и вызвана необходимостью официального подтверждения эффективности комплекса используемых на конкретном объекте информатизации мер и средств защиты информации.

При *аттестации объекта информатизации подтверждается* его соответствие требованиям по защите информации от несанкционированного доступа, в том числе от компьютерных вирусов, от утечки за счет побочных электромагнитных излучений и наводок при специальных воздействиях на объект (высокочастотное навязывание и облучение, электромагнитное и радиационное воздействие), от утечки или воздействия на нее за счет специальных устройств, встроенных в объекты информатизации.

Аттестация предусматривает комплексную проверку (аттестационные испытания) защищаемого объекта информатизации в реальных условиях эксплуатации с целью оценки соответствия применяемого комплекса мер и средств защиты требуемому уровню безопасности информации.

Аттестация проводится органом по аттестации в соответствии со схемой, выбираемой на этапе подготовки к аттестации из следующего основного перечня работ:

– анализ исходных данных по аттестуемому объекту информатизации;

– предварительное ознакомление с аттестуемым объектом информатизации;

– проведение экспертного обследования объекта информатизации и анализ разработанной документации по защите информации на этом объекте с точки зрения ее соответствия требованиям нормативной и методической документации;

– проведение испытаний отдельных средств и систем защиты информации на аттестуемом объекте информатизации с помощью специальной контрольной аппаратуры и тестовых средств;

– проведение испытаний отдельных средств и систем защиты информации в испытательных центрах по сертификации средств защиты информации по требованиям безопасности информации;

– проведение комплексных аттестационных испытаний объекта информатизации в реальных условиях эксплуатации;

– анализ результатов экспертного обследования и комплексных аттестационных испытаний объекта информатизации и утверждение заключения по результатам аттестации.

На этапе аттестационных испытаний объекта информатизации:

– осуществляется анализ организационной структуры объекта информатизации, информационных потоков, состава и структуры комплекса технических средств и программного обеспечения, системы защиты информации на объекте, разработанной документации и ее соответствия требованиям нормативной документации по защите информации;

– определяется правильность категорирования объектов электронно-вычислительной техники и классификации автоматизированных систем при их аттестации, выбора и применения сертифицированных и несертифицированных средств и систем защиты информации;

– проводятся испытания несертифицированных средств и систем защиты информации на аттестуемом объекте или анализ результатов их испытаний в испытательных центрах (лабораториях) по сертификации;

– проверяется уровень подготовки кадров и распределение ответственности персонала за обеспечение выполнения требований по безопасности информации;

– проводятся комплексные аттестационные испытания объекта информатизации в реальных условиях эксплуатации путем проверки фактического выполнения установленных требований на различных этапах технологического процесса обработки защищаемой информации;

– оформляются протоколы испытаний и заключение по результатам аттестации с конкретными рекомендациями по устранению допущенных нарушений, приведению системы защиты объекта информатизации в соответствии с установленными требованиями по совершенствованию этой системы, а также рекомендациями по контролю за функционированием объекта информатизации.

18.3. Порядок проведения служебных расследований

Порядок проведения служебных расследований инцидентов в случае реализации угроз информационной безопасности предприятия определяет организационные процедуры и правила информирования службы безопасности и руководства, установления причин инцидентов, выявления нарушителей и степени их вины, минимизации негативных последствий и предложения мер по устранению возможностей для реализации угроз в будущем. Установленные процедуры и правила должны строго соответствовать

действующему законодательству и внутренним нормативным документам предприятия.

Под *инцидентом* понимается любое нештатное событие при функционировании любого сервиса информационной технологии или осуществления бизнес-процесса в части нарушения конфиденциальности, целостности, доступности, имеющее умышленный или неумышленный характер. Инциденты нарушений безопасности подразделяются на события, связанные с реализацией конкретной угрозы, приводящей к потерям и необходимости затрат на восстановление и обнаруженные уязвимости. С целью планирования и минимизации потерь, а также упрощения процедур расследования составляется максимально возможный перечень угроз и рисков их реализации.

По каждому инциденту сотрудник службы безопасности, ответственный за мониторинг событий, формирует сообщение с указанием места инцидента, времени и даты, электронного адреса пораженного объекта; сведений об участниках, свидетелях, названии подразделения, задействованных или затронутых информационных активов, журнала событий и т.д.

В случае невозможности быстрого определения всей информации об инциденте она может быть занесена в базу данных позднее. Сообщение формируется на основании звонка, электронного письма или служебной записки, подготовленной обнаружившим инцидент сотрудником или руководителем структурного подразделения на имя руководителя службы безопасности.

Уровень инцидента в соответствии с утвержденным перечнем определяется руководителем службы безопасности, после чего инцидент считается зарегистрированным и начинается предварительный этап дополнительного сбора информации для подготовки соответствующего заключения. Должно быть установлено максимально возможное время регистрации и подготовки заключения, в том числе в случае обнаружения уязвимости с целью ее устранения в реальном масштабе времени. В заключении даются указания по изменению бизнес-процессов, настройке и конфигурированию технических средств, приобретению средств защиты и т.д.

В случае реализации угрозы для проведения детального расследования инцидента приказом руководителя предприятия создается комиссия, состоящая из опытных и квалифицированных сотрудников в составе не менее трех человек. В приказе о назначении комиссии дополнительно указывается: основание для проведения расследования инцидента; порядок наделения членов комиссии полномочиями по сбору, истребованию необходимых материалов, привлечению консультантов, экспертов и указания оказания содействия всеми службами и подразделениями предприятия для объективной оценки причин и ущерба; срок предоставления акта с материалами расследования и предложениями.

По каждому нарушению информационной безопасности должно быть собрано максимальное количество материалов, данных и сведений (доказательств), необходимых для последующего анализа определения причин инцидента и принятия мер правовой защиты интересов предприятия.

Доказательства в виде конкретных предметов обеспечиваются метками идентификации (дата, время, место изъятия, кто, где обнаружил доказательство). При хранении такие предметы и прежде всего электронные носители должны быть защищены от модификации и уничтожения. Опрос участников инцидента должен быть задокументирован в соответствующем протоколе.

Комиссия в ходе проведения расследования инцидента информационной безопасности наделяется следующими правами: доступа ко всем материалам, имеющим отношение к расследованию инцидента; приглашения на собеседование должностных лиц, обладающих информацией по существу проводимого расследования.

При этом комиссия обязана руководствоваться нормами законодательства; обеспечивать сохранность и конфиденциальность материалов, приобщаемых к акту о расследовании инцидента; выработать рекомендации и предложения о мерах юридической ответственности нарушителей, а также предложения по совершенствованию комплекса обеспечения информационной безопасности предприятия; оформить результаты расследования инцидента в виде акта с приложениями материалов расследования.

В процессе проведения расследования комиссия устанавливает наличие мероприятий по выполнению политики безопасности и поддерживающих ее нормативно-методических документов, причины нарушения, виновных лиц и другие факторы, способствующие реализации угрозы.

На основании акта комиссии руководителем предприятия принимается решение в соответствии с законодательством о защите интересов своего предприятия.

Контрольные вопросы

1. Дайте определение понятия «режимный объект» и видов обеспечения его безопасности.
2. Каковы цель и задачи организации пропускного режима?
3. Что является нормативной основой организации пропускного режима и каково ее общее содержание?
4. Что определяет порядок пропуска (прохода) физических лиц на территорию режимного объекта?
5. Что предусматривают правила въезда (выезда) транспортных средств на территорию режимного объекта?
6. Каковы особенности организации охраны режимного объекта?
7. Каковы суть и содержание нормативной основы организации охранных мероприятий?

8. Назовите действия охраны при тревоге и других чрезвычайных ситуациях.

9. Каковы цель и задачи организационного обеспечения внутриобъектового режима?

10. В чем состоит содержание организационного обеспечения режима секретности?

11. Каким образом организуется конфиденциальное делопроизводство?

12. Какие организационные процедуры включает обеспечение режима секретности?

13. Как организуется засекречивание сведений, составляющих государственную тайну?

14. Как организуются допуск и доступ к сведениям, составляющим государственную тайну?

15. Каковы правила обращения секретных документов?

16. Перечислите основные правила организации секретного делопроизводства.

17. Что предусматривает организационный режим делопроизводства и обращения документов с грифом «Для служебного пользования» (ДСП)?

18. Расскажите об особенностях современных систем автоматизированного документооборота.

19. В чем принципиальные отличия технологии workflow от традиционных систем автоматизации управленческой деятельности?

20. В чем состоит суть и содержание работ по противодействию технической разведке?

21. Дайте определение понятия «аттестация объектов информатизации».

22. Назовите основной перечень работ по аттестации объектов информатизации.

23. Каковы цель и задачи проведения служебных расследований инцидентов нарушений информационной безопасности?

24. Как проводится служебное расследование инцидентов при реализации угрозы информационной безопасности?

Глава 19

УПРАВЛЕНИЕ ПЕРСОНАЛОМ НА ПРЕДПРИЯТИЯХ И В ОРГАНИЗАЦИЯХ

19.1. Общие положения

Успешная деятельность любого предприятия (организации), в том числе по обеспечению информационной безопасности, зависит от *эффективного менеджмента* — вида деятельности по руководству людьми (персоналом), по использованию их опыта, квалификации, интеллекта и труда для достижения целей предприятия.

Эффективность менеджмента в области информационной безопасности зависит от таких факторов:

– как организационная структура системы обеспечения информационной безопасности предприятия, характеризуемая гибкостью (оперативностью реагирования на возникающие угрозы безопасности видам информации, имеющим ключевое значение для сохранения конкурентоспособности предприятия, его информационным и коммуникационным системам), комплексностью (учетом внешних и внутренних факторов воздействия на объекты информационной безопасности при формировании структуры системы обеспечения информационной безопасности), качеством управления и исполнения функций управления по обеспечению информационной безопасности;

– уровень, прогрессивности технических решений по обеспечению безопасности информации, применяемых на предприятии;

– выполнение положений законодательства и корпоративных нормативных актов в области обеспечения безопасности информации;

– качество персонала предприятия, характеризуемого прежде всего его лояльностью и квалификацией.

Эффективный менеджмент в области обеспечения информационной безопасности возможен только при условии успешного решения задач подбора и расстановки кадров, мотивации их труда и постоянного повышения квалификации в целях противодействия угрозам информационной безопасности.

19.2. Подбор и расстановка кадров

При подборе и расстановке кадров в области обеспечения информационной безопасности предприятия в первую очередь проводятся специальные мероприятия:

– учет вопросов конфиденциальности в традиционных кадровых методиках и процедурах приема и увольнения;

– подготовка нормативно-правовой базы по документированию добровольного согласия работника на определенное ограничение прав, связанное с дополнительным контролем его деятельности в целях обеспечения безопасности предприятия.

Наряду с традиционными кадровыми процедурами, обеспечивающими выполнение требований экономической эффективности бизнес-процессов, должны быть предусмотрены дополнительные меры, соответствующие принятой политике безопасности. К ним, в частности, относится учет личных и деловых качеств кандидата при решении вопроса о приеме на работу.

В качестве методической основы для подготовки соответствующих оценок могут быть использованы *организационные схемы* (*графы*). Узлы графов соответствуют определенным рабочим местам (должностям), на которые предполагается назначить кандидата, а дуги — информационным потокам, необходимым для его работы, с указанием ценности информации и соответствующей категории (грифа) ее защиты.

Существует два общих принципа, которые следует иметь в виду при разработке указанных организационных схем.

Первый принцип состоит в следующем: роль и ответственность исполнителей необходимо разделять таким образом, чтобы был обеспечен взаимоконтроль сотрудников за непрерывностью критически важных бизнес-процессов.

Второй принцип заключается в минимизации привилегий исполнителя, т.е. в предоставлении ему только тех прав доступа к нематериальным активам, которые необходимы для выполнения служебных обязанностей.

Хорошей практикой при подборе и расстановке кадров является разработка на основе организационных графов так называемых *профессиограмм*, в которых наряду с квалификационными требованиями и должностной инструкцией содержится перечень необходимых личных и деловых качеств кандидата, в том числе противопоказания, служащие мотивированным отказом от должности. Очевидно, что с точки зрения обеспечения безопасности личные качества кандидата имеют определенный приоритет по сравнению с профессиональными характеристиками.

При составлении профессиограмм следует обратить внимание на то, что в число противопоказаний не могут быть включены признаки расовой или этнической принадлежности кандидата, его религиозных или политических убеждений и взглядов, сексуальной ориентации и его семейного положения.

Профессиограмма является основой для начала взаимодействия с кандидатом, а также для обоснования особых условий его рабо-

ты, т.е. дополнительных мер контроля и соответствующего стимулирования, которые включают в трудовой контракт при достижении соглашения между кандидатом и работодателем.

В соответствии с трудовым законодательством нормативно-правовой основой для введения дополнительных ограничений по контролю за деятельностью персонала является соответствующая запись в уставе предприятия о необходимости выполнения требований по безопасности, а также пункты коллективного договора и правил внутреннего распорядка, согласованные с требованиями политики безопасности. Это обусловлено тем, что на основании Конституции Российской Федерации: «каждый имеет право на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени» и «каждый имеет право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений. Ограничение данного права допускается только на основании судебного решения». Данная норма не дает работодателю прямого основания для ограничения указанных прав даже в случае потенциальной возможности работы со сведениями, составляющими государственную тайну. Проблема решается путем оформления добровольного согласия кандидата в порядке, установленном внутренними нормативными документами предприятия. Отказ можно считать признаком проявления нелояльности кандидата и основанием для отказа ему в зачислении.

Дополнительные процедуры подбора кандидатов должны обеспечить составление достаточно полного психологического портрета кандидата, его морально-волевых качеств и возможных склонностей к противоправным действиям.

Полный объем таких процедур включает проведение следующих мероприятий.

Верификация сведений о кандидате — тщательное изучение и дополнительная документальная проверка биографических и других сведений, представляемых кандидатом в резюме, анкетах, справках, рекомендательных письмах и т.д. С согласия кандидата проводится также внешняя проверка по учетам правоохранительных органов, по месту жительства, местам предыдущей работы при неукоснительном соблюдении законодательства об оперативно-розыскной деятельности и защите персональных данных. Эти меры позволяют в достаточной степени исключить любые случаи предоставления заведомо ложных данных в целях мошенничества и завышения объективной оценки качеств кандидата. Любое выявленное в ходе проверки отклонение данных, представленных кандидатом, может рассматриваться как противопоказание для его зачисления. ***Оценка показателей возможной лояльности и благонадежности кандидата*** — важный фактор этой стадии отбора. Их условно делят на психологическую удовлетворенность, определяемую степенью нематериальной заинтересованности (люби-

мая работа, хорошие семейные отношения и т.д.), и экономическую, зависящую главным образом от размеров денежного вознаграждения. Очевидно, что указанная совокупность психологической и экономической удовлетворенности находится в достаточно жесткой связи и их оценка зависит от конкретной личности, ее ценностной ориентации и внешних обстоятельств. Тем не менее без информации внешнего характера получить достаточно достоверную характеристику возможной лояльности и благонадежности очень затруднительно.

Психологическое тестирование — использование относительно недорогих методов анализа ответов на специально разработанные в соответствии с достижениями психологической науки вопросники (тесты). На основе этих методов оцениваются такие качества личности, как психо-эмоциональная устойчивость, умственные способности, быстрота реакции на нестандартные ситуации и т.д. Однако, как и всякий подход к оценке человеческих качеств, методы психологического тестирования не дают полного описания личности и в особых случаях (для высшей категории персонала) подкрепляются другими методами исследований.

Графологическая экспертиза — заключение о личных качествах кандидата на основе исследования почерка, являющегося мощным признаком аутентификации личности. Однако данный метод, за исключением подтверждения подлинности собственноручной подписи (кроме мнения эксперта), пока не имеет хорошего обоснования верификации результатов экспертизы.

Психофизиологическое тестирование — исследование личных качеств кандидата путем анализа физиологических изменений (частоты пульса и дыхания, биоритмов, выделения кожных покровов и т.д.) испытуемого при ответах на вопросы, подготовленные и задаваемые экспертом (полиграфологом) по специально разработанным методикам. Физиологические реакции регистрируются датчиками, сигналы которых обрабатываются специальным прибором — полиграфом, более известным как «детектор лжи». Хотя никаких отечественных норм правового регулирования применения полиграфа пока не существует, метод получил достаточно широкое признание в практике антикриминального противодействия как в правоохранительных органах, так и в коммерческих структурах. Считается научно доказанным положение, что опрос с применением полиграфа в аспекте криминалистической экспертизы дает возможность объективного обнаружения и исследования хранящихся в памяти человека следов событий, имевших место в его жизни ранее, либо установления отсутствия таких следов. Экспериментально доказано, что следы событий, хранящиеся в эмоциональной памяти человека, практически неуничтожимы на протяжении всей жизни, по крайней мере на период удаления более чем в 20 лет.

Тем не менее применение полиграфа не является абсолютным методом доказательства преступлений, это частный метод криминалистической профилактики правонарушений, связанных с исполнением служебных обязанностей. Анализ природы явлений, лежащих в основе применения полиграфа для обнаружения скрываемой информации, показывает, что психофизиологическая экспертиза наиболее эффективна при ориентации на оценку достоверности сведений, представляемых испытуемым кандидатом, а в остальных случаях верификация результатов экспертизы достаточно затруднительна.

Каждый из выделенных методов проверки и исследования личных качеств кандидата в отдельности не достаточно эффективен, но их комплексное использование позволяет достигать относительной достоверности сведений о профессиональной пригодности, потенциальной лояльности и благонадежности кандидата, о его творческих способностях и возможности адекватной реакции в экстремальных условиях. Поэтому окончательное решение принимается лишь после серии неформальных собеседований с кандидатом его непосредственного руководителя как представителя работодателя, а также ответственных работников службы безопасности и кадрового подразделения.

Хорошей практикой является временное зачисление кандидата с испытательным сроком и организацией повседневного наблюдения за его деятельностью при выполнении конкретных обязанностей.

Даже краткий обзор методов и средств проверки личных и профессиональных качеств кандидата показывает, что выполнение полного объема процедур подбора с учетом требований обеспечения безопасности требует привлечения значительных ресурсов.

В целях снижения затрат на специальные дополнительные мероприятия целесообразно провести определенное ранжирование должностей по степени возможных угроз и рисков бизнес-процессов.

В зависимости от оценки критичности должности планируется соответствующая совокупность процедур отбора. Так, к высшей категории персонала, который должен пройти полный объем проверочных мероприятий, можно отнести руководство (топ-менеджеров), сотрудников службы безопасности, системных администраторов и администраторов информационной безопасности. К остальным категориям сотрудников можно применять меньший объем процедур проверки, что позволит снизить затраты на выполнение необходимых требований по безопасности.

Специалистами была проанализирована эффективность различных методов и процедур отбора кандидатов. Эффективность оцен-

Таблица 1. **Результаты сравнительного анализа эффективности различных методов и процедур отбора кандидатов**

Процедура	Профпригодность			Удовлетворенность	Лояльность	Криминальные наклонности	Криминальное прошлое	Аутентичность личности	Отдельные признаки	Интегративная эффективность
	Психологические качества	Умственные способности	Опыт работы							
Опрос	3	3	5	4	4	3	3	5	—	30
Внешняя проверка	2	4	5	5	5	5	3	4	—	33
Анкетные данные	2	3	4	3	3	2	3	3	2	25
Опрос с использованием полиграфа	2	2	3	4	5	3	5	5	5	34
Графологический анализ	5	—	—	3	4	4	—	5	—	21
Психологический тест	5	5	—	4	4	4	3	3	—	27
Собеседование	4	5	5	5	4	4	3	4	3	37
Наблюдение	3	3	3	1	—	3	—	4	3	20
Информация из БД учета	2	2	2	—	—	—	4	4	—	14
Опрос по месту жительства	1	—	1	2	3	2	2	3	1	15
Анализ медицинских данных	3	—	—	—	—	—	—	4	—	7

ки по каждой процедуре оценивалась по пятибалльной шкале, а интегральная эффективность представляет собой сумму частных оценок (табл. 1).

На основании подобных оценок можно произвести выбор совокупности необходимых процедур в зависимости от категории персонала, отбираемого с учетом выполнения требований обеспечения безопасности.

Все приведенные выше процедуры могут быть использованы не только при подборе кандидатов, но и на всем протяжении «жизненного цикла» деятельности сотрудников на данном предприятии. Возможно проведение внеплановых проверок в случае

появления признаков аномальной активности, при перемещении на другую должность и т.д. Важным условием их проведения является четкое выполнение норм трудового законодательства.

Серьезное внимание при управлении персоналом в аспекте обеспечения безопасности необходимо обратить на активное участие служб безопасности в процедурах ***увольнения сотрудников***, особенно по инициативе администрации. Очевидно, что любое увольнение независимо от его причины таит в себе явные угрозы, связанные, в частности, с утечкой значимой информации и/или неправомерным использованием интеллектуальной собственности. Существующее законодательство о труде не дает каких-либо правовых оснований для проведения дополнительных мероприятий специального характера, а мотивация к добровольному сотрудничеству, как правило, отсутствует, за исключением обязательств, принятых на себя работником при приеме на работу или в ходе трудовой деятельности.

До объявления окончательного решения об увольнении по инициативе администрации должна быть проведена дополнительная оценка риска от возможных правонарушений и приняты меры по минимизации возможного ущерба. Лишь с учетом этих сведений может быть принято окончательное решение об увольнении, обязательным элементом которого должно стать собеседование увольняемого с ответственными сотрудниками службы безопасности и кадровых структур. В ходе собеседования в доброжелательной форме работнику напоминают о принятых обязательствах и возможных мерах юридической ответственности. Иногда в качестве одной из дополнительных мер защиты организационного характера рекомендуется оформление в ходе увольнения официальной подписки о неразглашении конфиденциальных сведений. Однако это возможно в случае, если такая процедура была предусмотрена особыми условиями контракта при приеме на работу, но и тогда эффективность ее использования в судебной практике защиты интересов работодателя очень низкая.

При увольнении работника по собственному желанию риск должен оцениваться с учетом истинных причин увольнения, что предполагает дополнительное изучение характера взаимоотношений сотрудника с коллегами, результативности его деятельности, семейного положения, наличия конфликтов личного или служебного характера. Лишь после этого даются рекомендации по удержанию данного работника в коллективе либо по реализации процедуры бесконфликтного увольнения.

19.3. Мотивация добросовестной деятельности

Регулярное изучение поведения наиболее ответственных категорий персонала, понимание интересов и потребностей сотруд-

ников, мотивов их поведения и выбор соответствующих методов стимулирования добросовестной деятельности являются одной из неотъемлемых составляющих управления персоналом, именуемой *мотивацией сотрудников*. Мотивация есть создание внутреннего побуждения к нужным действиям, что особенно актуально для службы безопасности. Данная служба является одним из наиболее важных, но тем не менее вспомогательных подразделений, не имеющих прямого отношения к реализации основных бизнес-процессов предприятия.

Стимулы как внешние побуждения к проявлению тех или иных мотивов деятельности могут быть моральные, духовные, материальные, физические, а оптимальный результат мотивации дает их органичное сочетание. Мотивация деятельности конкретного работника определяется сложной совокупностью его потребностей и интересов, которые постоянно меняются и могут существенно различаться даже внутри одной организации. Для того чтобы эффективно мотивировать своих работников, руководителю следует достаточно точно знать, каковы на самом деле их потребности и интересы в настоящее время, и на этой основе обеспечивать возможность удовлетворения интересов работников при условии эффективного выполнения ими должностных обязанностей. Решению такой задачи может способствовать использование так называемого метода *оценки деятельности подчиненных*, являющегося основополагающим во всей системе методов стимулирования.

Эта оценка предполагает определение субъектом управления (руководителем) результативности деятельности управляемого объекта (подчиненных) на основе анализа соответствия выполняемой работы заданным требованиям, например установленным политикой безопасности. Как метод мотивации оценка должна обязательно сопровождаться доведением ее результатов до подчиненных сотрудников. Такое условие отражает естественную потребность каждого человека в признании важности и полезности его труда, в желании получить достойную оценку своих действий, поведения, знаний, профессионализма.

Важной формой контроля деятельности сотрудников является их периодическая или даже внеплановая аттестация, которая служит коллективной формой оценки. Для ряда должностей, в частности государственных служащих, такая процедура предусмотрена в действующем законодательстве. Хорошей практикой является применение аналогичных процедур аттестации к категории персонала, имеющей высший показатель критичности в аспекте обеспечения безопасности.

Результативность деятельности и соответствующая оценка может быть как положительной, так и отрицательной. С учетом этого в системе мер мотивации можно выделить меры положительного и отрицательного стимулирования.

Метод ***положительного стимулирования*** ориентирован на развитие позитивных качеств работника и удовлетворение его внутренних интересов. Его суть состоит в использовании различных форм поощрения: премирования, объявления благодарности, вручения различных наград, присвоения званий, повышения в должности и т.п. В теории и практике управления принято считать, что поощрение — наиболее действенное средство мотивации и стимулирования.

Любая форма поощрения должна быть обоснована, понятна коллективу и самому работнику и, как правило, не должна иметь регулярный характер, а быть привязанной к конкретным достижениям и результатам.

Суть метода ***отрицательного стимулирования*** составляет применение различных форм порицания (наказания), включая меры дисциплинарно-административного принуждения. Такой метод наиболее широко используется в практике работы службы безопасности как надзорного органа в общей системе управления предприятием. Порицание осуществляется в виде устного осуждения, неодобрения поведения или результативности действий сотрудника. К дисциплинарным мерам воздействия относится официальное объявление в форме приказа замечания, выговора, предупреждения о неполном служебном соответствии, отмены непредусмотренных законом должностных льгот. Крайней мерой дисциплинарного взыскания является увольнение сотрудника с соблюдением всех норм трудового законодательства, которое, как уже указывалось, отражает интересы наемных работников, а не работодателей, давая исчерпывающий и достаточно краткий перечень оснований для увольнения. Тем не менее в случае правильного оформления внутренних нормативных документов (устав, коллективный договор, правила внутреннего распорядка, должностные инструкции) в аспекте обеспечения безопасности возможно и увольнение за нарушение требований безопасности.

Практика управления персоналом свидетельствует о том, что метод отрицательного стимулирования оказывает более сильное, чем поощрение, эмоциональное воздействие, поэтому его применение эффективно лишь в случае достаточной обоснованности порицания, которое выносится с учетом конкретной ситуации и психического состояния человека, его индивидуальных особенностей и доводится до сведения работника в тактичной и доброжелательной форме. В противном случае возникает вероятность появления нового внутреннего нарушителя. Поэтому при выборе меры взыскания следует проявлять особую тщательность, взвешивая такие факторы, как размер ущерба, возможность исправления недостатков, результативность деятельности в целом данного работника, его репутация в коллективе и возможное воспитательное воздействие наказания на остальных членов коллектива.

Наиболее часто метод отрицательного стимулирования используется в форме критики, которая дает возможность порицания действий работника в режиме реального времени «по горячим следам» без применения мер дисциплинарного взыскания, которые возможны лишь на уровне первого руководителя предприятия. Степень и направленность критических высказываний могут быть различными — от доброжелательных замечаний и пожеланий до «разноса» в присутствии других подчиненных. Специалисты насчитывают до 25 форм критических высказываний, что свидетельствует о широком диапазоне возможной мотивации. Важным условием получения положительного результата критики является соблюдение принципа равных возможностей, иными словами, критикуемый должен иметь право на изложение своей позиции и на внимательное, объективное отношение к обсуждаемым действиям.

Кроме оценки деятельности конкретного сотрудника к методам коллективной мотивации относится создание так называемых ориентирующих условий. Это предполагает наличие здорового психологического климата или обстановки, которая способствует проявлению разумной инициативы и творческого подхода к выполнению поставленных задач, и в то же время обеспечивает нетерпимость к равнодушию, безынициативности, нарушениям установленных правил служебных взаимодействий и дисциплины.

Создание *ориентирующих условий* предполагает:

– неукоснительное соблюдение руководителем норм законодательства о труде, положений трудового договора, норм по технике безопасности и охране труда, правил внутреннего распорядка;

– создание реальных и гласных условий стимулирования сотрудников в зависимости от конкретных результатов их деятельности;

– обеспечение неотвратимости и обоснованности применения дисциплинарно-административных форм принуждения за нарушение работником своих должностных обязанностей;

– заинтересованное участие в решении личных затруднений сотрудников, включая бытовые вопросы;

– обеспечение гарантий юридической, а в ряде случаев и физической защиты при наличии угроз криминального характера.

Как и всякий механизм управления персоналом, мотивация обладает высокой степенью неопределенности с точки зрения разработки типовых перечней мероприятий и тем более их содержания. Поэтому чрезвычайно важно обеспечить из существующего многообразия практическое применение максимально возможной совокупности методов и средств стимулирования, поскольку использование одних методов в ущерб другим, как правило, дает отрицательные результаты.

В проблеме мотивации, как, впрочем и во всей проблеме обеспечения информационной безопасности, важную роль играет та-

кой механизм управления персоналом, как постоянное самообучение и периодическое повышение квалификации.

В то же время известно: чтобы обучение было эффективным, ему должны предшествовать процедуры мотивации. Сотрудники из числа критических категорий персонала должны ясно представлять себе необходимость обучения, в том числе в аспекте обеспечения безопасности. Обычно и мотивация и разъяснение необходимости обучения вызывают определенное отторжение у работников, занятых в области основной деятельности предприятия, так как создают определенные трудности и помехи. Поэтому ведущим условием должно стать стремление работников к развитию своих профессиональных знаний, умений и навыков, нацеленное на реализацию интересов в работе на данном предприятии. В этом механизме управления персоналом не существует простых типовых решений, но имеется определенная система оказания образовательных услуг, помогающая решать проблему развития кадрового потенциала предприятия (организации) в области обеспечения информационной безопасности.

19.4. Организация подготовки кадров в области обеспечения информационной безопасности

Важным направлением деятельности по обеспечению информационной безопасности является подготовка кадров, которую проводят:

– образовательные учреждения федеральных органов исполнительной власти, решающие в основном традиционные задачи защиты информации, в первую очередь, от внешних угроз;

– образовательные учреждения Минобрнауки России, осуществляющие подготовку специалистов по широкому кругу вопросов создания защищенных информационных систем, а также технических и программных средств защиты информации;

– негосударственные образовательные учреждения, в том числе региональные.

Образовательная деятельность в указанной области осуществляется по специальностям, объединенным в перечне направлений подготовки (специальностей) высшего профессионального образования в отдельную группу «Информационная безопасность». В состав этой группы входят следующие специальности: «Криптография» — 090101; «Компьютерная безопасность» — 090102; «Организация и технология защиты информации» — 090103; «Комплексная защита объектов информатизации» — 090104; «Комплексное обеспечение информационной безопасности автоматизированных систем» — 090105; «Информационная безопасность телекоммуникационных систем» — 090106; «Противодействие техническим разведкам» — 090107.

Образовательная деятельность в рассматриваемой области имеет следующие направления:

– подготовка специалистов с высшим образованием (7 специальностей; квалификации — математик, специалист по защите информации; срок обучения 5 или 5,5 лет);

– подготовка специалистов со средним профессиональным образованием (одна специальность; квалификация — техник; срок обучения — 2 года 10 месяцев);

– повышение квалификации специалистов с высшим образованием (72 и более учебных часов);

– предоставление возможности получения дополнительной квалификации (до 500 учебных часов);

– переподготовка специалистов с высшим образованием (более 500 учебных часов);

– подготовка кадров высшей квалификации — кандидатов и докторов наук по специальности «Методы и системы защиты информации, информационная безопасность» по отраслям физико-математических, технических и юридических наук.

Наибольшее количество специалистов подготавливается по специальностям «Организация и технология защиты информации» — 090103, «Комплексная защита объектов информатизации» — 090104, «Комплексное обеспечение информационной безопасности автоматизированных систем» — 090105 и «Информационная безопасность телекоммуникационных систем» — 090106.

Объектами профессиональной деятельности специалиста по защите информации по специальности «Организация и технология защиты информации» являются правовое обеспечение, организация и эксплуатация систем и средств обеспечения защиты информации на объектах информатизации. Выпускник этой специальности в соответствии с фундаментальной и специальной подготовкой может заниматься экспериментально-исследовательской, проектной, организационно-управленческой и эксплуатационной деятельностью, выполнять работы, связанные с обеспечением комплексной защиты информации на основе разработанных программ и методик, разрабатывать предложения по совершенствованию существующих методов и средств защиты информации, участвовать в обследовании объектов защиты, их аттестации и категорировании, разрабатывать проекты нормативных и методических материалов, регламентирующих работу по защите информации.

Специальность «Комплексная защита объектов информатизации» связана с разработкой и использованием методов, средств и систем обеспечения защиты информации на объектах информатизации. Выпускники занимаются исследованием причин возникновения, форм проявления, возможности параметризации и оценки опасности физических явлений, увеличивающих

вероятность нежелательного воздействия на информационные процессы в защищаемом объекте, составляют методики расчетов и программ экспериментальных исследований по технической защите информации, проектируют и внедряют комплексные системы и отдельные специальные технические и программно-математические средства защиты информации на объектах информатизации, обеспечивают организационные и инженерно-технические меры защиты информационных систем, осуществляют техническое обслуживание средств защиты информации, участвуют в проведении аттестации объектов, помещений, технических средств, программ, алгоритмов на предмет соответствия требованиям защиты информации по соответствующим классам безопасности.

Студенты, обучающиеся по специальности «Комплексное обеспечение информационной безопасности автоматизированных систем», ориентированы на решение проблем, связанных с построением, исследованием и эксплуатацией систем и технологий обеспечения информационной безопасности автоматизированных систем, в том числе обеспечения комплексной безопасности распределенных информационных банковских систем. Объектами профессиональной деятельности выпускников являются автоматизированные системы обработки, хранения и передачи информации определенного уровня конфиденциальности, методы и средства обеспечения информационной безопасности автоматизированных систем. Видами профессиональной деятельности являются: проектно-конструкторская; организационно-технологическая; экспериментальная; организационно-управленческая.

Объекты профессиональной деятельности специалиста по защите информации по специальности «Информационная безопасность телекоммуникационных систем» — методы, средства и системы обеспечения информационной безопасности телекоммуникационных систем. Специалист по защите информации в соответствии с фундаментальной и специальной подготовкой может заниматься разработкой моделей информационной безопасности телекоммуникационных систем, построением и анализом защищенных систем и сетей передачи информации, сопровождением разработки технического обеспечения систем информационной безопасности, организационно-правовым и инженерно-техническим обеспечением защиты информации.

Контрольные вопросы

1. Чем определяется эффективность менеджмента в области информационной безопасности?
2. Опишите суть и содержание использования организационных схем и профессиограмм при подборе кадров.

3. Что является нормативно-правовой основой для введения дополнительных ограничений по контролю за деятельностью персонала?

4. Перечислите организационные процедуры для составления психологического портрета работника.

5. В чем состоят особенности верификации сведений о работнике при его приеме на работу?

6. Дайте описание методов психологического тестирования и графологической экспертизы.

7. Опишите специфику использования метода психофизиологического тестирования.

8. Какова цель ранжирования должностей по степени риска управления бизнес-процессами?

9. Опишите участие службы безопасности в процедурах увольнения сотрудников.

10. Дайте определение мотивации как метода управления персоналом.

11. Опишите суть и содержание метода положительного стимулирования.

12. В чем состоят особенности метода отрицательного стимулирования.

13. Что предполагает создание ориентирующих условий?

14. Что определяет актуальность вопросов самообучения и повышения квалификации?

15. Перечислите основные специальности, по которым осуществляется подготовка кадров в области обеспечения информационной безопасности, и основные направления образовательной деятельности в этой области.

СПИСОК ЛИТЕРАТУРЫ

К главе 1

Белл Д. Грядущее постиндустриальное общество. Опыт социального прогнозирования / пер. под ред. В.Л. Иноземцева. — М., 1999.

Гейтс Б. Дорога в будущее. — М., 1994.

Зиновьев А.А. На пути к сверхобществу. — М.: Центрполиграф, 2000.

Иноземцев В.Л. К теории постэкономической общественной формации. — М., 1995.

Иноземцев В.Л. Современное постиндустриальное общество: природа, противоречия, перспективы. — М.: Логос, 2000.

Тоффлер О. Третья волна. — М., 1995.

Чоговадзе Г Г. Информация. Общество. Человек. — М.: Дата+, 2003.

К главе 2

Бачило И.Л. Информационное право. Основы практической информатики. — М.: Изд-во Тихонова М.Ю., 2001.

Войниканис Е.А. Информация. Собственность. Интернет / Е.А. Войниканис, М.В. Якушев. — М.: Волтерс Клувер, 2004.

Городов О.А. Основы информационного права России. — СПб., 2003.

Лапина М.А. Информационное право / М.А. Лапина [и др.]. — М.: Юнити-Дана, 2004.

Рассолов М.М. Информационное право. — М.: Юристъ, 1999.

Стрельцов А.А. Обеспечение информационной безопасности России. Теоретические и методологические основы. — М.: МЦНМО, 2002.

Фисун А.П. Право и информационная безопасность / А.П. Фисун [и др.] — М.: Приор, 2005.

К главе 3

Возженников А.В. Национальная безопасность: теория, политика, стратегия. — М.: РАГС, 1998.

Основы национальной безопасности России / под ред. В.Л. Манилова. — М.: Друза. 1998.

Прохожев А.А. Национальная безопасность: основы теории, сущность, проблемы. — М.: РАГС, 1997.

Прохожев А.А. Человек и общество: законы социального развития и безопасности. — М.: РАГС, 2002.

Стрельцов А.А. Обеспечение информационной безопасности России. Теоретические и методологические основы. — М.: МЦНМО, 2002.

К главе 4

Грачев Г. В. Информационно-психологическая безопасность личности: состояние и возможности психологической защиты. — М.: Институт психологии РАН, 1996.

Пярин В. А. Безопасность электронного бизнеса / В. А. Пярин [и др.]. — М.: Гелиос-АРВ, 2002.

Расторгуев С. П. Философия информационной войны. — М.: Autopan, 2000.

Стрельцов А. А. Правовое обеспечение информационной безопасности России. Теоретические и методологические основы. — Минск: Беллітфонд, 2005.

Теория и практика обеспечения информационной безопасности / под ред. П. Д. Зегжды. — М.: Яхтсмен, 1996.

К главе 5

Алексеев С. С. Право: азбука, теория, философия: Опыт комплексного исследования. — М.: Статут, 1999.

Морозова Л. А. Основы государства и права. — М.: Московский независимый институт международного права, 1997.

Общая теория государства и права. Академический курс. Т. 2. Теория права. — М.: Зерцало, 1998.

Шумилов В. М. Правоведение. — М.: ТК Велби, Проспект, 2006.

К главе 6

Конституция Российской Федерации от 12 декабря 1993 года.

Стрельцов А. А. Правовое обеспечение информационной безопасности России. Теоретические и методологические основы. — Минск: Беллітфонд, 2004.

Туманова Л. В.. Обеспечение и защита права на информацию / Л. В. Туманова, А. А. Снытников. — М.: Городец, 2001.

Фатьянов А. А. Правовое обеспечение безопасности информации в Российской Федерации. — М.: Юрист, 2001.

Фисун А. П. Право и информационная безопасность / А. П. Фисун [и др.]. — М.: Приор, 2005.

К главе 7

Бачило И. Л. Информационное право / И. Л. Бачило [и др.]. — СПб.: Юридический центр, 2001.

Войниканис Е. А. Информация. Собственность. Интернет / Е. А. Войниканис, М. В. Якушев. — М.: Волтерс Клувер, 2004.

Фатьянов А. А. Правовое обеспечение безопасности информации в Российской Федерации. — М.: Юрист, 2001.

Федеральный закон «Об информации, информационных технологиях и защите информации» от 27 июля 2006 г.

Якушев М. А. К вопросу об обновлении российского информационного законодательства // Развитие правового обеспечения информационной безопасности. — М.: Престиж, 2005.

К главе 8

Федеральный закон «О персональных данных» от 27 июля 2006 г.

К главе 9

Гражданский кодекс Российской Федерации. Часть четвертая.

Колятин В. О. Интеллектуальная собственность (Исключительные права). — М.: Норма, 2000.

Фисун А. П. Право и информационная безопасность / А. П. Фисун [и др.]. — М.: Приор, 2005.

К главе 10

Фатьянов А. А. Правовое обеспечение безопасности информации в Российской Федерации. — М.: Юрист, 2001.

Федеральный закон «О коммерческой тайне» от 29 июля 2004 года.

Фисун А. П. Право и Интернет. Информационная безопасность / А. П. Фисун [и др.]. — М.: Приор, 2005.

К главе 11

Государственная тайна и ее защита в Российской Федерации / под ред. М. А. Вуса и А. В. Федорова. — СПб.: Юридический центр «Пресс», 2003.

Закон Российской Федерации «О государственной тайне» от 21 июля 1993 г.

Северин В. А. Правовое обеспечение информационной безопасности предприятия. — М.: Городец, 2000.

К главе 12

Соловьяненко Н. И. Об электронном документе и электронной подписи // Развитие правового обеспечения информационной безопасности. — М.: Престиж, 2005.

Федеральный закон «Об электронной цифровой подписи» от 10 января 2002 г.

К главе 13

Федеральный закон «О техническом регулировании» от 27 декабря 2002 г.

К главе 14

Аверкин А. Е. Нарушение авторских, смежных, изобретательских и патентных прав / А. Е. Аверкин [и др.]. — М.: Книга сервис, 2002.

Гражданский кодекс Российской Федерации. Часть первая.
Гражданский процессуальный кодекс Российской Федерации.
Кодекс Российской Федерации об административных правонарушениях.
Фисун А. П. Право и информационная безопасность / А. П. Фисун [и др.]. — М.: Приор, 2005.
Уголовный кодекс Российской Федерации.
Уголовно-процессуальный кодекс Российской Федерации.

К главе 15

Безлепкин Б. Т. Судебная система, правоохранительные органы и адвокатура России. — М.: Юристъ, 2001.
Дмитриев Ю. А. Правоохранительные органы / Ю. А. Дмитриев, М. А. Шапкин. — М.: Мастерство, 2002.
Федеральный конституционный закон «О судебной системе Российской Федерации» от 31 декабря 1996 г.
Федеральный конституционный закон «О военных судах Российской Федерации» от 23 июня 1999 г.
Федеральный конституционный закон «Об арбитражных судах в Российской Федерации» от 28 апреля 1995 г.
Федеральный закон «О мировых судьях в Российской Федерации» от 17 декабря 1998 г.
Федеральный закон «О третейских судах в Российской Федерации» от 24 июля 2002 г.

К главе 16

Курило А. П. Обеспечение информационной безопасности бизнеса / А. П. Курило [и др.]. — М., БДЦ-пресс, 2005.
Стрельцов А. А. Правовое обеспечение информационной безопасности России. Теоретические и методологические основы. — Минск: Беллітфонд, 2004.

К главе 17

Зегжда Д. П. Как построить защищенную информационную систему / Д. П. Зегжда, А. М. Ивашко. — СПб.: НПО «Мир и семья-95», 1997.
Курило А. П. Обеспечение информационной безопасности бизнеса / А. П. Курило [и др.]. — М.: БДЦ-пресс, 2005.
Медведовский И. Д. Атака через Интернет / И. Д. Медведовский [и др.]. — СПб.: НПО «Мир и семья-95», 1997.
Пярин В. А. Безопасность электронного бизнеса / В. А. Пярин [и др.]. — М.: Гелиос АРВ, 2002.

К главе 19

Лукичева Л. И. Управление персоналом. — М.: Омега-Л, 2007.
Маслоу А. Г. Мотивация и личность / пер. с англ. А. М. Татлыбаевой. — СПб.: Евразия, 2001.

ОГЛАВЛЕНИЕ

ЧАСТЬ III
ОРГАНИЗАЦИОННОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Учебное издание

Стрельцов Анатолий Александрович,
Горбатов Виктор Сергеевич,
Полякова Татьяна Анатольевна и др.

Организационно-правовое обеспечение информационной безопасности

Учебное пособие

Редактор *Н. А. Соколова*
Технический редактор *Е. Ф. Коржуева*
Компьютерная верстка: *Н. А. Рогоза*
Корректор *Г. Н. Петрова*

Изд. № 101112145. Подписано в печать 28.06.2007. Формат 60×90/16.
Гарнитура «Таймс». Печать офсетная. Бумага офсетная № 1. Усл. печ. л. 16,0.
Тираж 2 500 экз. Заказ № 25728.

Издательский центр «Академия». www.academia-moscow.ru
Санитарно-эпидемиологическое заключение № 77.99.02.953.Д.004796.07.04 от 20.07.2004.
117342, Москва, ул. Бутлерова, 17-Б, к. 360. Тел./факс: (495)330-1092, 334-8337.

Диапозитивы предоставлены издательством.

Отпечатано в ОАО «Саратовский полиграфкомбинат».
410004, г. Саратов, ул. Чернышевского, 59. www.sarpk.ru

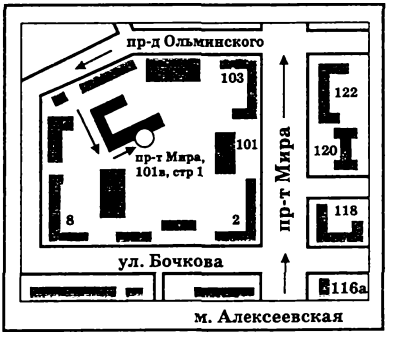
Издательский центр «Академия»

Учебная литература для профессионального образования

НАШИ КНИГИ МОЖНО ПРИОБРЕСТИ (ОПТОМ И В РОЗНИЦУ)

МОСКВА

129085, Москва,
пр-т Мира, д. 101 в, стр. 1
(м. Алексеевская)
Тел./факс: (495) 648-0507,
330-1092, 334-1563
E-mail: sale@academia-moscow.ru



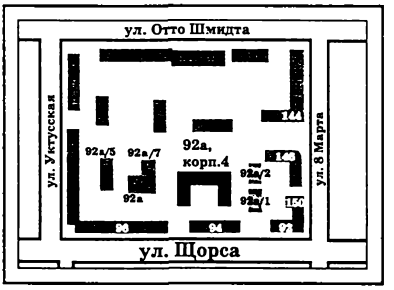
ФИЛИАЛЫ:

СЕВЕРО-ЗАПАДНЫЙ

198020, Санкт-Петербург,
наб. Обводного канала,
д. 211-213, литер «В»
Тел.: (812) 251-9253, 252-5789, 575-3229
Факс: (812) 251-9253, 252-5789
E-mail: fspbacad@peterstar.ru

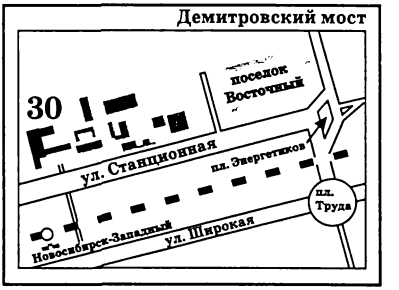
ПРИВОЛЖСКИЙ

603005, Нижний Новгород,
ул. Алексеевская, д. 24г и 24д
Тел.: (8312) 34-1158, 18-0404
Факс: (8312) 18-1678
E-mail: pf-academia@bk.ru



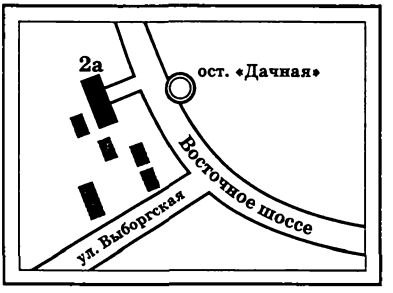
УРАЛЬСКИЙ

620144, Екатеринбург,
ул. Щорса, д. 92а, корп. 4
Тел.: (343) 257-1006
Факс: (343) 257-3473
E-mail: academia-ural@mail.ru



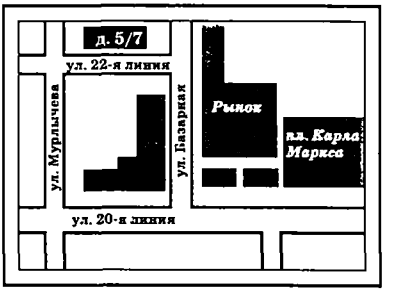
СИБИРСКИЙ

630108, Новосибирск,
ул. Станционная, д. 30
Тел. / факс: (383) 300-1005
E-mail: academia_sibir@mail.ru



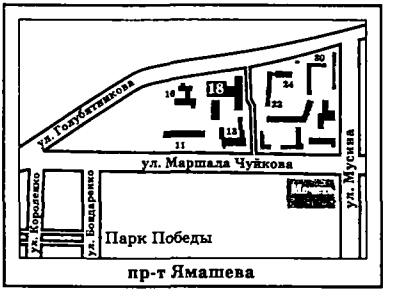
ДАЛЬНЕВОСТОЧНЫЙ

680014, Хабаровск, Восточное шоссе, д. 2а
Тел. / факс: (4212) 27-6022
E-mail: filialdv-academia@yandex.ru



ЮЖНЫЙ

344037, Ростов-на-Дону,
ул. 22-я линия, д. 5/7
Тел.: (863) 253-8566;
Факс: (863) 251-6690
E-mail: academia-rostov@skytc.ru



ПРЕДСТАВИТЕЛЬСТВО В РЕСПУБЛИКЕ ТАТАРСТАН

420094, Казань,
Ново-Савиновский район,
ул. Голубятникова, д. 18
Тел. / факс: (843) 520-7258, 556-7258
E-mail: academia_kazan@mail.ru

Для студентов учреждений высшего профессионального образования. Может быть полезно специалистам в области защиты информации.

В. П. МЕЛЬНИКОВ, С. А. КЛЕЙМЕНОВ, А. М. ПЕТРАКОВ
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ
Под ред. С. А. Клейменова
Объем: 336 с.

В учебном пособии представлены основные положения, понятия и определения обеспечения информационной безопасности деятельности общества, его различных структурных образований, организационно-правового, технического, методического, программно-аппаратного сопровождения. Особое внимание уделено проблемам методологического обеспечения деятельности как общества, так и конкретных фирм и систем (ОС, СУБД, вычислительных сетей), функционирующих в организациях и фирмах. Описаны криптографические методы и программно-аппаратные средства обеспечения информационной безопасности, их защиты от излучения, вирусного заражения, разрушающих программных действий и изменений.

Для студентов учреждений высшего профессионального образования.

В. В. ПЛАТОНОВ
ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ВЫЧИСЛИТЕЛЬНЫХ СЕТЕЙ
Объем: 240 с.

В учебном пособии рассмотрены удаленные сетевые атаки и организация защиты от них. Изложены методы описания атак, их классификация и основные тенденции развития. Описаны основные технологии межсетевых экранов, вопросы их оценки и тестирования. Проанализированы методы построения систем обнаружения вторжений, их разновидности и перспективы. Рассмотрены про-

блемы защиты при организации удаленного доступа, принципы построения и функционирования виртуальных ведомственных сетей (VPN), а также основные отечественные средства для их построения.

Для студентов учреждений высшего профессионального образования.

С. П. РАСТОРГУЕВ
ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
Объем: 192 с.

В учебном пособии рассмотрены понятия национальной безопасности; виды безопасности; информационная безопасность (ИБ) в системе национальной безопасности Российской Федерации; основные понятия, общеметодологические принципы теории ИБ; анализ угроз ИБ, проблемы информационной войны; государственная информационная политика; проблемы региональной информационной безопасности; виды информации; методы и средства обеспечения ИБ; методы нарушения конфиденциальности, целостности и доступности информации; причины, виды, каналы утечки и искажения информации.

Для студентов учреждений высшего профессионального образования.

П. Б. ХОРЕВ
МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ В КОМПЬЮТЕРНЫХ СИСТЕМАХ
Объем: 256 с.

В учебном пособии основное внимание уделяется программным и программно-аппаратным методам и средствам защиты информации. Рассматриваются, в частности, модели безопасности, используемые в защищенных версиях операционной системы Windows (в том числе использование функций криптографического интерфейса приложений CryptoAPI) и в операционных системах «клона» Unix.

Для студентов учреждений высшего профессионального образования. Может быть полезно специалистам в области информационной безопасности.