ПОЛИТЕХ
Инженерно-строительный институт

ПОЛИТЕХ
Санкт-Петербургский политехнический университет Петра Великого

ПОЛИТЕХ-ПРЕСС

В. В. Глухов А. И. Зайцев А. Н. Братушка

ЗАЩИТА ГОСУДАРСТВЕННОЙ ТАЙНЫ В РОССИЙСКОЙ ФЕДЕРАЦИИ: ПОНЯТИЯ, ОРГАНИЗАЦИЯ, ПРАВИЛА, ОТВЕТСТВЕННОСТЬ

Учебное пособие

Министерство науки и высшего образования Российской Федерации

САНКТ-ПЕТЕРБУРГСКИЙ
ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ ПЕТРА ВЕЛИКОГО

В. В. Глухов А. И. Зайцев А. Н. Братушка

ЗАЩИТА ГОСУДАРСТВЕННОЙ ТАЙНЫ В РОССИЙСКОЙ ФЕДЕРАЦИИ: ПОНЯТИЯ, ОРГАНИЗАЦИЯ, ПРАВИЛА, ОТВЕТСТВЕННОСТЬ

Учебное пособие

ПОЛИТЕХ-ПРЕСС
Санкт-Петербургский
политехнический университет
Петра Великого

Санкт-Петербург
2020

ББК 67я73
Г55

Р е ц е н з е н т ы:
Доктор технических наук, профессор ВШТБ СПбПУ *В. Г. Бурлов*
Кандидат технических наук, доцент, доцент ВШТБ СПбПУ *С. В. Ефремов*

Глухов В. В. **Защита государственной тайны в Российской Федерации: понятия, организация, правила, ответственность** : учеб. пособие / В. В. Глухов, А. И. Зайцев, А. Н. Братушка. – СПб. : ПОЛИТЕХ-ПРЕСС, 2020. – 240 с.

В современном мире – мире свободного обмена информацией – все более обостряется необходимость сохранения отдельных направлений деятельности государства в целом, а также министерств, ведомств, учреждений, предприятий.

Ограничения вводятся на поиск, получение, хранение, обмен информацией, составляющих государственную, коммерческую и персональную тайну.

Дается толкование и комментарии положений действующего российского законодательства о государственной тайне, анализируется практика его применения.

Рассматриваются система документов по защите государственной тайны, порядок засекречивания и рассекречивания сведений, составляющих государственную тайну, основные положения по лицензированию деятельности организаций на проведение работ, связанных с использованием сведений, составляющих государственную тайну, ответственность должностных лиц за нарушение законодательства в области защиты государственной тайны.

Предназначено студентам, аспирантам, руководителям государственных и негосударственных структур, специалистам в сфере защиты информации, преподавателям учебных заведений.

Ил. 31. Библиогр.: 22 назв.

Печатается по решению
Совета по издательской деятельности Ученого совета
Санкт-Петербургского политехнического университета Петра Великого.

ISBN 978-5-7422-7028-7
doi:10.18720/SPBPU/2/id20-101

Ministry of Science and Higher Education of the Russian Federation

PETER THE GREAT ST. PETERSBURG
POLYTECHNIC UNIVERSITY

V. V. Glukhov A. I. Zaitsev A. N. Bratushka

PROTECTION OF STATE SECRETS IN THE RUSSIAN FEDERATION: NOTIONS, ORGANIZATION, RULES, RESPONSIBILITY

Training manual

POLYTECH-PRESS
Peter the Great
St.Petersburg Polytechnic
University

Saint-Petersburg
2020

Reviewers:
Doctor of Engineering, professor at the Graduate School of
Technosphere Safety of SPbPU *V. G. Burlov*
Candidate (PhD) of Engineering, associate professor,
associate professor at the Graduate School of Technosphere Safety of SPbPU
S. V. Efremov

Glukhov V. V. **Protection of state secrets in the Russian Federation: notions, organization, rules, responsibility**: training manual / V. V. Glukhov, A. I. Zaitsev, A. N. Bratushka. – St. Petersburg: POLYTECH-PRESS, 2020. – 240 p.

In the modern world - the world of free exchange of information - the necessity of preserving certain activities of the state as a whole, as well as ministries, departments, institutions, and enterprises is becoming more and more urgent.

Restrictions are imposed on search, acquisition, storage, and exchange of the information that constitutes state, commercial, and personal secrets.

The manual provides interpretation and commentary on the provisions of Russia's current legislation on state secrets and analyzes its application.

The authors consider the system of documents for protecting state secrets, the order of classifying and declassifying information constituting state secrets, the basic provisions for licensing activities of organizations for work related to the use of information constituting state secrets, the responsibility of officials for violations of legislation in the field of protection of state secrets.

The manual is intended for students, postgraduate students, heads of state and non-state structures, specialists in the sphere of information protection, teachers of educational institutions.

Figures 31. References: 22 titles.

Printed by the Publishing Council
of the Peter the Great St. Petersburg polytechnic university Academic Council

ISBN 978-5-7422-7028-7
doi:10.18720/SPBPU/2/id20-101

Подушка, на которой спит полководец,
не должна знать его мыслей.

М. И. Кутузов

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Лучше всего хранятся в тайне секреты,
которые никого не интересуют.

Кармен Сильва

В истории человечества такие понятия, как государственная измена, шпионаж и разглашение государственной тайны, существуют тысячелетия.

Противозаконная разведывательная деятельность предполагает похищение официально засекреченной информации (государственной тайны) спецслужбами других государств любыми путями как напрямую через завербованных лиц, так и по техническим средствам разведки.

Меры уголовного наказания за шпионаж и государственную измену достаточно высокие, но это не останавливает изменников Родины. В настоящее время эти преступления совершаются не по политическим мотивам, а с экономической целью.

С 2000 г. в России арестовано более 40 противозаконно работающих на иностранные государства, пресечена деятельность почти 200 сотрудников спецслужб других государств.

Безопасность – одна из характеристик и условий функционирования и развития социальных, экономических, технических, экологических и биологических систем. Это – одна из фундаментальных потребностей социума. На уровне общественного сознания понятие «безопасность» трактуется как отсутствие опасности, сохранность, надежность, конкурентоспособность.

В широком смысле *безопасность рассматривается как гарантия существования и устойчивости развития* объектов социальной природы, является атрибутивной характеристикой, выделяемой, наблюдаемой и оцениваемой социальными субъектами. Состояние безопасности во многом определяют зрелость общества, степень осознания им угроз, реальных источников опасности.

Понятие «безопасность» чрезвычайно емкое, поэтому при анализе проблематики обычно выделяют ряд сфер безопасности: государственную, социальную, экономическую, общественную, военную, криминогенную и др. В государственно организованном обществе в качестве основных объектов безопасности выделяются человек, общество, регион и государство.

Основным *субъектом обеспечения безопасности* является государство, осуществляющее функции в этой области через органы законодательной, исполнительной и судебной властей. Для обеспечения безопасности в социальной системе исключительную важность имеет нормальное функционирование государственно-правовых институтов. Государственное управление является поддерживающим и стабилизирующим фактором защитных реакций социальных субъектов.

Общим, характерным для всех областей жизнедеятельности человека и общества является то, что *безопасность как цель*, условие и стратегия защиты от опасности нацелена в конечном счете на выживание социальной системы, личности, общества и государства. Однако необходимо отметить, что система обеспечения безопасности не сводится только к пассивной безопасности, например защите. Безопасность должна предполагать активность, учет состояния объекта воздействия со стороны угрозы, упреждающую реакцию.

В наше время на глазах одного поколения внедрение современных информационных технологий привело к коренному изменению образа жизни и качества труда многих людей, а информационные ресурсы стали одним из решающих факторов развития личности, общества и государства. Интенсивное внедрение средств информатизации, телекоммуникации и связи в жизнь

человека и связанная с этим глобализация процессов общественного развития существенно увеличили зависимость общества, отдельных сфер его жизнедеятельности от процессов производства, распространения и использования информации, а также обусловили превращение ее в объект разнообразных общественных отношений. Страны с более развитой информационной инфраструктурой, устанавливая технологические стандарты и предоставляя потребителям свои ресурсы, де-факто определяют условия формирования и деятельности информационных инфраструктур в других странах, оказывают воздействие на развитие их информационной сферы. Вследствие этого в промышленно развитых странах сегодня при формировании национальной политики приоритет получают развитие средства защиты и обеспечение безопасности информационной сферы.

Процессы формирования информационного общества оказывают воздействие на многие элементы государственности, затрагивают как национальные, так и международные системы социальных регуляторов отношений государств, народов, юридических и физических лиц. Поэтому главы государств, подписавшие в 2000 г. в Окинаве Хартию глобального информационного общества, констатировали, что усилия, направленные на его развитие, «должны сопровождаться согласованными действиями по созданию безопасного и свободного от преступности киберпространства».

Возрастающие ценность информации и ее роль в общественных процессах, а также концентрация информации в компьютерных системах диктуют необходимость ее адекватной защиты, в том числе и посредством формирования определенных правовых механизмов. Вследствие этого на рубеже веков обострилась и стала одной из основных глобальных проблем всего человечества *проблема обеспечения информационной безопасности*. При этом помимо традиционных задач защиты информации все острее проявляется необходимость постановки и решения задач защиты от деструктивной информации.

Безопасность, согласно ее законодательно закрепленному определению, рассматривается как *один из видов защищенности*.

Следует, однако, еще раз заметить, что безопасность не всегда обеспечивается только защитой. Социологи подчеркивают, что пониманию безопасности как защищенности должен быть присущ институциональный подход, акцентирующий внимание на внутренних механизмах поддержания устойчивого, сбалансированного развития системы. Так, например, информационная безопасность может быть достигнута соответствующими правилами поведения и взаимодействия объектов, высокой профессиональной подготовкой персонала, безотказностью работы техники, надежностью всех видов обеспечения функционирования объектов безопасности и т. д.

Учебное пособие подготовлено по курсу «Защита государственной тайны» в соответствии с требованиями Федерального закона «О защите государственной тайны».

Состав материала сформирован на основе требований, предъявляемых к специалистам по защите информации, составляющей государственную тайну.

По результатам освоения учебного материала необходимо знать вопросы: законодательство Российской Федерации в области защиты государственной тайны; основные требования нормативно-методических документов по режиму секретности, противодействию иностранным техническим разведкам и защите информации от утечки по техническим каналам и условия выполнения этих требований; порядок отнесения сведений к государственной тайне, их засекречивание и рассекречивание; порядок организации защиты информации, составляющей государственную тайну на предприятии; планирование и финансирование работ по комплексной защите информации, составляющей государственную тайну; организация лицензирования деятельности предприятий, учреждений и организаций в области защиты государственной тайны; организация защиты государственной тайны при проведении совместных работ; организация работы по комплексной защите информации на объектах, предъявляемых для деятельности иностранных инспекций, на совместных предприятиях, при научно-техническом и экономическом сотрудничестве

с зарубежными странами; обеспечение информационной безопасности предприятия (организации) в средствах массовой информации; ответственность за правонарушения в области защиты государственной тайны.

Пособие может быть использовано студентами – магистрами и аспирантами, изучающими специальный или факультативный курс «Защита государственной тайны», а также для подготовки и повышения квалификации руководителей и специалистов предприятий по вопросам защиты информации, составляющей государственную тайну.

Глава 1

ИЗ ИСТОРИИ ШПИОНАЖА

Кто чего не знает, то для него тайна;
все сокрытое, неизвестное, неведомое.

В. И. Даль

Практически на всем протяжении истории нашей страны уникальные природные ресурсы и мощный интеллектуальный потенциал русского народа всегда притягивали в Россию иностранных разведчиков, что заставляло создать и постоянно совершенствовать службы разведки и контрразведки. «Зело берегитесь шпионов на Воронеже» – произнес Петр I в 1703 г.

Первое упоминание о защите секретов в российском законодательстве содержится в Генеральном регламенте (указ Петра I «О делах тайности подлежащих» от 13 января 1724 г.) разглашение государственной тайны было отнесено к государственным преступлениям, и основным в нем было наказание «в виде вырывания ноздрей, а также вечная ссылка с лишением сословных привилегий и конфискацией имущества».

Список деяний, относящихся к государственной измене, фигурирует в упоминании об уголовных и исправительных наказаниях 1845 г. Более детальный перечень определяло Уголовное уложение 1903 г., где устанавливалась ответственность за снятие копий с секретных документов, а также за шпионство, хотя само это понятие еще не имело юридической трактовки.

Контрразведывательная служба была создана в том же 1903 г. Проводя первые мероприятия в этом направлении, Разведочное отделение Главного штаба сразу столкнулось с проблемой защиты государственной тайны. Полная беспечность и безответственность царских властей привели к тому, что шпионаж проник в Генеральный штаб и в министерства. Усилиями германских и австрийских спецслужб были созданы шпионские организации в среде российской аристократии.

Например, получение Д. И. Менделеевым бездымного пороха хорошего качества заставило работать разведки мира над поиском технологии его изготовления. Ученый настаивал на секретности рецептуры и производстве только на частных заводах, но процесс так и не засекретили, и порох самого высокого качества начали изготавливать за рубежом.

Впрочем, сам Дмитрий Иванович технологию изготовления получил, можно сказать, шпионским способом. Во Франции он начал вести учет количества вагонов с азотом, серной кислотой, спиртом, кислородом и готовой продукции, поступавших на пороховой завод. Исходя из этого, ученый сделал пропорциональный расчет состава бездымного пороха.

Хорошо известна работа шпионской сети кайзеровской Германии в России, которая велась под прикрытием коммерческой деятельности фирмы «Зингер и К^0». Продавая швейные машинки, агенты фирмы работали коммивояжерами во всех российских губерниях. При этом они решали разнообразные разведывательные задачи, в том числе:

– изучение обслуживаемых и других местных дорог, их проходимость;

– предоставление несколько раз в течение года особых списков населенных пунктов с точным указанием числа дворов и жителей;

– поиск данных о расположении воинских частей, складов;

– сбор сведений о заводах, фабриках, что они производят, численность рабочих.

Вся информация передавалась в немецкий Генеральный штаб через искровой телеграф, расположенный на Невском проспекте российской столицы в доме 28/21 – «Дом Зингера».

Целенаправленно, не жалея денежных средств, с конца XIX века работала японская разведка. В разное время Страна восходящего солнца имела в России более тысячи промышленных и военных шпионов.

Так, в начале 1900-х в Одессе в одном из ресторанов, куда часто заходили ужинать морские офицеры, работал поваром некий Ясуно-суки Ямомото (кадровый морской офицер). Будто бы не понимая русского языка, он периодически выходил в зал, спрашивал: «Хорошо?» – и при этом внимательно слушал хмельные разговоры офицеров. Гуляя по набережной, определял типы кораблей как военных, так и гражданских, изучал их возможности. В целом он получил полную информацию о русской эскадре Черноморского флота.

С началом строительства Россией Транссибирской железнодорожной магистрали под благовидным предлогом проехал на коне всю Сибирь профессиональный разведчик, военный атташе в Берлине барон Фукусима Ясумаса. Он собрал информацию не только о скоростных и грузовых возможностях трассы по ходу маршрута, но и обо всех военных частях. В результате представил отчет на 800 стр.

Перед началом Русско-японской войны 1904–1905 гг. в России действовало более пятисот японских шпионов. Они добывали сведения, работая продавцами в приобретенных ими лавках, фотографами, прачками, санитарами в военных госпиталях (рис. 1.1).

В 1904 г. в Петербурге были арестованы два японских морских офицера, много лет служивших в крупной коммерческой фирме. Один из них принял православие, женился на русской девушке, исполнял все церковные обряды.

Следует отметить, что в России работало 439 фирм и предприятий с австро-венгерским капиталом, которые были вовлечены в шпионскую деятельность.

Например, разведывательным отделением Варшавского военного округа за период с 1901 по 1911 г. была раскрыта деятельность 150 иностранных шпионов, однако до суда удалось довести только 17 дел, по которым привлекли к ответственности 33 человека, из них четверых оправдали.

Рис. 1.1. Пойманный японский шпион
(Маньчжурия, 1904 г.)

Вербовка граждан России осуществлялась в основном подкупом. По идеологическим соображениям российские подданные шли на предательство в единичных случаях. Большинство из них служило в штабах, на крупных заводах и фабриках. Например, старший адъютант штаба Восточного военного округа подполковник Гримм привлек писарей для снятия копий секретных документов, а для маскировки их передачи использовал жену.

Директор Сестрорецкого оружейного завода генерал-майор Дмитриев-Бойцуров стал шпионом, совершив крупную денежную растрату. Директор Путиловской судоверфи Оренский передал в германский Генеральный штаб судостроительные программы на 1912–1930 гг., технические условия по морскому кораблестроению и на поставку металла на Петербургский военный завод. Никто даже не обратил внимания, что Оренский является германским подданным.

При аресте отставного корнета Унгерн фон Штенберга были изъяты документы и «Секретный доклад комиссии по обороне и величине новобранцев в призыв 1910 г.». В 1910 г. английский журнал «Инжиниринг» поместил подробные чертежи русских броненосцев «Гангут», «Полтава», «Севастополь», «Петропавловск», разумеется, украденные.

Полковник Штейн похитил крупную сумму казенных денег и за вознаграждение иностранной разведкой пытался передать секретные карты Генерального штаба. Был арестован бывший матрос Поваже, служивший брошюровщиком в типографии морского ведомства, который передавал вражеским агентам сборники флажных сигналов.

5 июля 1912 г. вступил в силу закон, расширивший понятие государственной измены. Вводился ряд новых карательных санкций. Было дано определение гостайны применительно к военной сфере. В июле 1914 г. вышел указ «Об утверждении Временного положения о военной цензуре» – «перечень сведений и изображений, касающихся внешней безопасности России», разглашение которых подлежало уголовному наказанию. В него, в частности, были включены посещения монаршими особами театра военного действия. Позже в перечень внесли запрет на распространение в печати и в публичных собраниях любых сведений о царской семье.

Меры, усиливавшие режим секретности, продвигались медленно и часто не соответствовали динамично менявшейся обстановке.

Список секретных сведений был законодательно принят 27 апреля 1926 г. Он содержал 12 пунктов и был разбит на три раздела – сведения военного, экономического характера и «иного рода». К государственной тайне были отнесены сведения о дислокации, организации, оборудовании, снабжении воинских частей, мобилизационных и оперативных планах, состоянии военной промышленности, «изобретение новых технических и иных средств военной обороны», состояние казначейских валютных фондов, переговорах с иностранными государствами, методах борьбы со шпионажем и контрреволюцией, шифрах и пр. Многие из этих понятий сохраняются в списке госсекретов до настоящего времени.

В современной России защита государственных секретов регулируется Конституцией РФ (ст. 29 ч. 4), федеральными законами «О государственной тайне» от 21.07.1993 и «О безопасности» от 28.12.2010.

Контрольные вопросы

1. Роль секретов в истории человечества.
2. В чем различие понятий «Шпионаж» и «Разведка»?
3. Виды и цели шпионажа в различные эпохи развития государств.
4. Выгоды шпионажа для государств с древних времен.
5. Шпионы как торговцы, дипломаты, работники сфер обслуживания.
6. Методы, способы добывания необходимых сведений для государства в древней истории.
7. Методы, способы сбора конфиденциальной информации в современном мире.
8. Основные области современного шпионажа:
   – природные ресурсы;
   – общественное мнение по отношению к внутренней и внешней политике государства;
   – стратегические, экономические области преимущества государства;
   – разведка военного потенциала;
   – операции контрразведки.
9. Историческая хронология основных этапов развития шпионажа.
10. Законность слежения (шпионажа), организованного государством.
11. История шпионажа в России от Ивана Грозного и противодействия ему.
12. Использование на практике библейских историй шпионажа.

Глава 2

ЗАЩИТА ИНФОРМАЦИИ, СОСТАВЛЯЮЩЕЙ ГОСУДАРСТВЕННУЮ ТАЙНУ

Не говори своему другу того,
что не должен знать твой враг.

Артур Шопенгауэр

2.1. Роль государственной тайны в национальной безопасности России

Отнесение тех или иных сведений к защите информации, государственной тайне продиктовано необходимостью обеспечения безопасности государства, что влечет за собой законодательное ограничение права граждан, закрепленного в ст. 29 (ч. 1, 4) Конституции Российской Федерации о том, что каждому гарантируется свобода мысли и слова. Каждый имеет право свободно искать, получать, передавать, производить и распространять информацию *любым законным способом*. Эта же статья содержит указание на то, что перечень сведений, составляющих защиту информации, определяется федеральным законом.

Отсутствие такого ограничения (указанного права граждан) в конечном счете поставило бы под угрозу возможность осуществления ими других своих прав (например, право на жизнь, на защиту частной собственности), само существование Российского государства, сделало бы невозможным обеспечение

государственной защиты прав и свобод граждан (ст. 45 Конституции Российской Федерации).

К основным объектам безопасности относятся:

– личность – ее права и свободы;

– общество – его материальные и духовные ценности;

– государство – его конституционный строй, суверенитет и территориальная целостность (рис. 2.1).

Понятие обеспечения безопасности государства весьма широко. Имеется в виду обеспечение безопасности в военной сфере, в сфере науки и техники, экономической безопасности, безопасности во внешнеполитической и внешнеэкономической деятельности РФ, безопасности в разведывательной, контрразведывательной и оперативно-розыскной деятельности.

Государство призвано защищать своих граждан, себя, свой конституционно-правовой строй от каких-либо посягательств как внешних, так и внутренних врагов. Одним из главных методов такой государственной защиты является отнесение сведений из той или иной сферы к государственной тайне, их засекречиванием (или рассекречиванием) и защитой. В связи с этим возникают правовые отношения.

Рис. 2.1. Структура национальной безопасности

Правоотношения порождают взаимные права и обязанности участвующих в них сторон. Например, отнесение сведений к государственной тайне влечет обязанность должностных лиц, государственных органов, имеющих к ним доступ, и граждан, получивших к ним доступ, не разглашать эти сведения неопределенному кругу лиц.

Эти правовые отношения возникают между органами государственной власти РФ, должностными лицами этих органов, органами государственной власти субъектов РФ, органами местного самоуправления и гражданами РФ, органами государственной власти иностранными государствами, их государственными органами и должностными лицами, иностранными гражданами и лицами без гражданства.

Такие правоотношения могут возникнуть и при заключении международного договора, по которому Россия передает сведения, составляющие государственную тайну, иностранному государству, а то в свою очередь обязуется не разглашать эти сведения и использовать их только в тех целях, для которых они переданы.

Главной целью законодательства о защите информации является задача избежать возникновения угрозы для национальной безопасности Российской Федерации. Угроза безопасности есть совокупность условий и факторов, создающих опасность жизненно важным интересам личности, общества или государства.

Реальная и потенциальная угроза объектам безопасности, исходящая от внутренних и внешних источников опасности, должна определять содержание деятельности по обеспечению внутренней и внешней безопасности. Поэтому главным при решении вопроса об отнесении сведений к защите информации, принятии мер по ее защите является правильная оценка возможной угрозы объекту безопасности и принятие адекватных мер по их нейтрализации.

В качестве защищаемой информации выступают защищаемые государством сведения в области его военной, внешнеполитической, контрразведывательной, экономической деятельности, распространение которых может нанести ущерб безопасности Российской Федерации.

Указанные сведения, в соответствии с Законом Российской Федерации от 21.07.1993 № 5485-1 «О государственной тайне», составляют государственную тайну и защищаются государством всеми доступными ему методами.

2.2. Система документов по защите государственной тайны

Тайной не пребудет слово.
Есть тайна двух, но тайны нет у трех,
И всем известна тайна четырех.

Абулькасим Фирдоуси

Документы по защите государственной тайны подразделяются на правовые, организационно-распорядительные, нормативные и плановые.

Правовые вопросы защиты государственной тайны закрепляются в самостоятельных правовых документах или отражаются в виде отдельных положений правовых документов более общего характера.

В правовых документах определяют концептуальные, правовые, организационные и экономические основы защиты государственной тайны:

– основные направления государственной политики в области защиты государственной тайны;

– основные права и обязанности государства, организаций, предприятий и граждан в области защиты государственной тайны;

– основные органы государственной власти, ответственные за организацию защиты государственной тайны, сфера их компетентности;

– основные правила и процедуры аттестации объектов и сертификации средств защиты информации, а также средств контроля состояния защиты информации;

– основные правила и процедуры лицензирования деятельности в области защиты государственной тайны и разработки средств защиты информации;

– виды и формы ответственности организаций, предприятий и граждан за нарушение требований по защите государственной тайны;

– финансово-экономические основы обеспечения работ по защите государственной тайны.

Рис. 2.2. Система документов в области защиты государственной тайны

Рис. 2.3. Основные правовые документы в области защиты государственной тайны

Структура правовых документов Российской Федерации в области защиты государственной тайны представлена на рис. 2.2, 2.3, 2.4.

К основному закону в области защиты информации и государственной тайны относится закон «О государственной тайне», а также более общие правовые акты: Конституция Российской Федерации, Гражданский и Уголовный кодексы Российской Федерации, законы «Об органах Федеральной службы безопасности в Российской Федерации»; «О порядке выезда из Российской Федерации и въезда в Российскую Федерацию» и др.

Организационно-распорядительные документы определяют состав и регламентируют деятельность соответствующих органов и служб при организации и осуществлении защиты государственной тайны.

По характеру регламентируемых вопросов и продолжительности действия организационно-распорядительные документы подразделяют на два вида:

– руководящие;

– распорядительные.

Руководящие документы помимо самостоятельного использования служат основой при разработке нормативных и плановых документов. Они являются подзаконными актами, детализирующими и раскрывающими положения правовых документов, устанавливают основные направления, единые принципы, порядок организации защиты государственной тайны соответствующими органами и службами с приведением их долговременных задач, функций, прав, обязанностей и мер ответственности.

Основными видами руководящих документов по защите государственной тайны являются: концепции, положения, руководства, наставления, инструкции, правила (рис. 2.5).

Положения по защите государственной тайны издаются на основе правовых актов и принятых концепций по защите и детализируют указанные документы в основном по вопросам

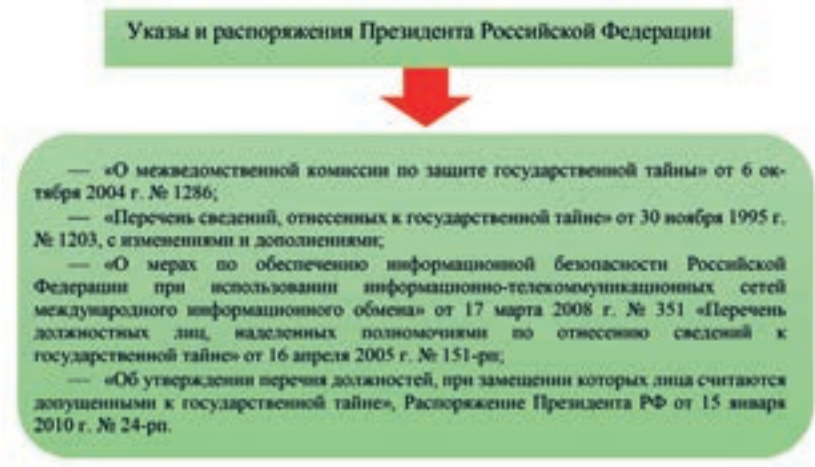

Рис. 2.4. Указы и распоряжения Президента Российской Федерации в области защиты информации и государственной тайны

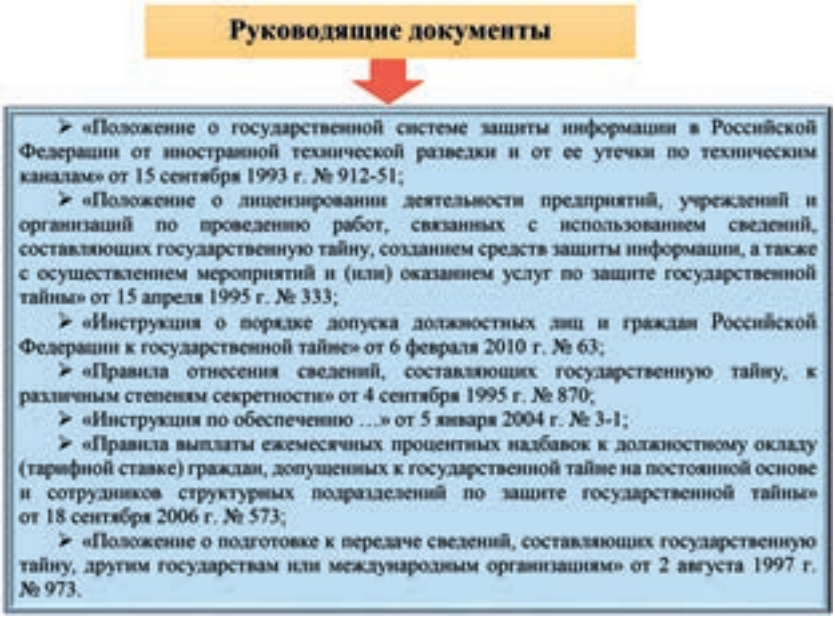

Рис. 2.5. Перечень основных руководящих документов в области защиты информации, составляющей государственную тайну

организации защиты государственной тайны в конкретном органе государственной власти (ведомстве) и, в частности, регламентируют:

– основные направления работ по защите государственной тайны;

– структуру органов и служб, ответственных за организацию и осуществление защиты государственной тайны, их права и обязанности;

– порядок организации и проведения типовых работ по защите государственной тайны для основных объектов защиты;

– финансово-экономические вопросы обеспечения работ по защите государственной тайны;

– вопросы государственного лицензирования в области защиты государственной тайны и др.

Также могут издаваться Положения об органах по защите государственной тайны и Положения о структурных подразделениях по защите государственной тайны на предприятиях и в организациях.

Детальные разъяснения отдельных практических вопросов по организации и осуществлению защиты государственной тайны включаются в соответствующие инструкции и правила.

Правовые и организационно-распорядительные документы носят нормативный характер, вводятся в действие правовым актом, являются обязательными для исполнения, поэтому эти два вида документов также обозначают общим термином «*нормативные правовые акты по защите государственной тайны*».

Распорядительные документы – документы текущего управления издают во исполнение или в дополнение к основополагающим документам и устанавливают направления, методы (способы, приемы) организации работ по защите государственной тайны в зависимости от возникающих конкретных задач управления и условий защиты государственной тайны. Основными видами распорядительных документов по защите государственной тайны являются решения, приказы, директивы, распоряжения, указания.

Нормативные документы устанавливают единые требования, нормы и правила защиты информации, составляющей государственную тайну, обязательные для исполнения в пределах установленной при их введении сферы действия и области их распространения.

Основными видами нормативных документов, в которых регламентируются вопросы защиты государственной тайны, являются:

– специальные нормативные документы ФСБ России, ФСТЭК России и других органов государственной системы защиты информации;

– нормативные документы государственной системы стандартизации.

Наряду с государственными стандартами отдельные вопросы защиты информации для различных объектов защиты регламентируются в стандартах отраслей, предприятий, а также в технических

условиях на отдельные виды продукции и в других нормативных документах.

Видами *специальных нормативных документов по защите информации* являются:

– нормы (например, требования эффективности защиты от технических разведок);

– модели, методики и методические указания (например, оценки возможностей технических средств разведки, эффективности мероприятий по защите, контроля и др.);

– рекомендации (пособия, например, по способам и средствам защиты от технических разведок и др.);

– лицензии предприятиям на право осуществления работ по защите информации;

– сертификаты соответствия средств защиты информации и средств контроля эффективности ее защиты требованиям в области защиты государственной тайны;

– аттестаты на объекты защиты информации.

Плановые документы включают целевые программы и планы в области защиты государственной тайны или соответствующие разделы программ и планов более общего характера, по которым осуществляется самостоятельное финансирование.

2.3. Закон «О государственной тайне»

Секрет – это не то, о чём не говорят никому.
Секрет – это то, о чём говорят наедине и вполголоса.

Марсель Паньоль

Закон РФ от 21.07.1993 № 5485-1 «О государственной тайне» определяет понятие государственной тайны как защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-разыскной деятельности, распространение которых

может нанести ущерб безопасности Российской Федерации. Таким образом, тайной может стать определенная информация, которая может передаваться как в устной, письменной, так и цифровой электронной форме. Эта информация подлежит государственной защите, представляющей собой систему норм, правил, ограничений, предписывающих различным лицам, имеющим допуск к государственной тайне, не разглашать и не передавать эту информацию лицам, не имеющим к ней допуск, под страхом наказания за нарушение данных запретов.

Кроме понятия государственная тайна в Законе «О государственной тайне» используются следующие *основные понятия*:

– носители сведений, составляющих государственную тайну, – материальные объекты, в том числе физические поля, в которых сведения, составляющие государственную тайну, находят свое отображение в виде символов, образов, сигналов, технических решений и процессов;

– система защиты государственной тайны – совокупность органов защиты государственной тайны, используемых ими средств и методов защиты сведений, составляющих государственную тайну, и их носителей, а также мероприятий, проводимых в этих целях;

– допуск к государственной тайне – процедура оформления права граждан на доступ к сведениям, составляющим государственную тайну, а предприятий, учреждений и организаций – на проведение работ с использованием таких сведений;

– доступ к сведениям, составляющим государственную тайну, – санкционированное полномочным должностным лицом ознакомление конкретного лица со сведениями, составляющими государственную тайну;

– гриф секретности – реквизиты, свидетельствующие о степени секретности сведений, содержащихся в их носителе, проставляемые на самом носителе и (или) в сопроводительной документации на него;

– средства защиты информации – технические, криптографические, программные и другие средства, предназначенные для защиты сведений, составляющих государственную тайну, средства,

в которых они реализованы, а также средства контроля эффективности защиты информации.

Перечень сведений, составляющих государственную тайну, – совокупность категорий сведений, в соответствии с которыми сведения относятся к государственной тайне и засекречиваются на основаниях и в порядке, установленных федеральным законодательством.

Вопросы, связанные с данными понятиями, рассмотрены в Законе «О государственной тайне» и получили дальнейшее развитие в постановлениях Правительства Российской Федерации, решениях Межведомственной комиссии по защите государственной тайны, документах министерств и ведомств, организаций.

Закон регулирует отношения, возникающие в связи с отнесением сведений к государственной тайне, их засекречиванием или рассекречиванием и защитой в интересах обеспечения безопасности Российской Федерации.

Государственная защита тайны обеспечивается законодательными органами Российской Федерации; Президентом Российской Федерации; Правительством Российской Федерации; органами государственной власти Российской Федерации; органами государственной власти субъектов Российской Федерации и органами местного самоуправления во взаимодействии с органами защиты государственной тайны, расположенными в пределах соответствующих территорий; органами судебной власти.

К органам защиты государственной тайны относятся:

– межведомственная комиссия по защите государственной тайны;

– 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;

– 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

Рис. 2.6. Структура системы защиты информации, составляющей государственную тайну в Российской Федерации

государственной тайны, функции которых определяются указанными руководителями в соответствии с нормативными документами, утверждаемыми Правительством Российской Федерации, и с учетом специфики проводимых ими работ (рис. 2.6).

Защита государственной тайны является видом основной деятельности органа государственной власти, предприятия, учреждения или организации.

Засекречивание сведений

Основанием для засекречивания является отнесение сведений к государственной тайне в соответствии с Перечнем сведений, составляющих государственную тайну, определяемым Законом «О государственной тайне», руководителями органов государственной власти в соответствии с Перечнем должностных лиц, наделенных полномочиями по отнесению сведений к государственной тайне, утверждаемым Президентом Российской Федерации.

Руководители, которые наделены полномочиями по отнесению сведений к государственной тайне, в соответствии с Перечнем сведений, отнесенных к государственной тайне, разрабатывают развернутые перечни сведений, подлежащих засекречиванию (рис. 2.7).

В эти перечни включаются сведения, полномочиями по распоряжению которыми наделены соответствующие руководители органов государственной власти.

Целесообразность засекречивания таких перечней определяется их содержанием. Указанные органы устанавливают 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.

Должностные лица, наделенные полномочиями по отнесению сведений к государственной тайне, вправе принимать решения

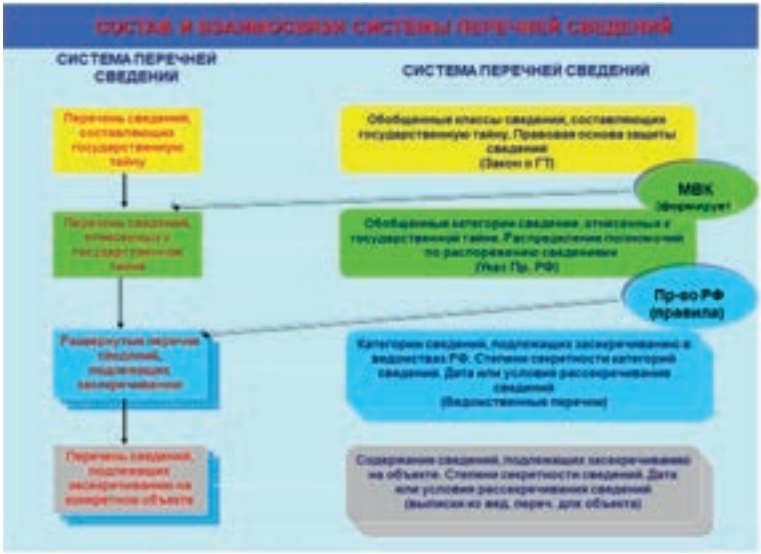

Рис. 2.7. Система формирования перечней сведений, составляющих государственную тайну

о засекречивании информации, находящейся в собственности предприятий, учреждений, организаций и граждан (далее – собственник информации), если эта информация включает сведения, перечисленные в Перечне сведений, отнесенных к государственной тайне.

Таким образом, основанием для засекречивания сведений является попадание их в развернутые перечни сведений, подлежащих засекречиванию.

В соответствии с Законом «О государственной тайне» *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, воинских формирований и органов, предусмотренных Федеральным законом «Об обороне», об их боевой и мобилизационной готовности, о создании и об использовании мобилизационных ресурсов;

– о планах строительства Вооруженных Сил Российской Федерации, других войск Российской Федерации, о направлениях развития вооружения и военной техники, о содержании и результатах выполнения целевых программ, научно-исследовательских и опытно-конструкторских работ по созданию и модернизации образцов вооружения и военной техники;

– о разработке, технологии, производстве, об объемах производства, о хранении, об 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;

– о тактико-технических характеристиках и возможностях боевого применения образцов вооружения и военной техники, о свойствах, рецептурах или технологиях производства новых видов ракетного топлива или взрывчатых веществ военного назначения;

– о 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 этих объектов;

– о 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 и ее отдельных регионов 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 обороноспособности и безопасности государства;

– о силах и средствах гражданской обороны, о дислокации, предназначении и степени защищенности объектов административного управления, о степени обеспечения безопасности населения, о функционировании транспорта и связи в Российской Федерации в целях обеспечения безопасности государства;

– об объемах, о планах (заданиях) государственного оборонного заказа, о выпуске и поставках (в денежном или натуральном выражении) вооружения, военной техники и другой оборонной продукции, о наличии и наращивании мощностей по их выпуску, о связях предприятий по кооперации, о разработчиках или об изготовителях указанных вооружения, военной техники и другой оборонной продукции;

– о достижениях науки и техники, о научно-исследовательских, об опытно-конструкторских, о проектных работах и технологиях, имеющих важное оборонное или экономическое значение, 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;

– о 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-разыскной деятельности, а также в области противодействия терроризму и в области обеспечения безопасности лиц, в отношении которых принято решение о применении мер государственной защиты*:

– о силах, средствах, об источниках, о методах, планах и результатах разведывательной, контрразведывательной, оперативно-разыскной деятельности и деятельности по противодействию терроризму, а также данные о финансировании этой деятельности, если эти данные раскрывают перечисленные сведения;

– о силах, средствах, об источниках, о методах, планах и результатах деятельности по обеспечению безопасности лиц, в отношении которых принято решение о применении мер государственной защиты, данные о финансировании этой деятельности, если эти данные раскрывают перечисленные сведения, а также отдельные сведения об указанных лицах;

– о лицах, сотрудничающих или сотрудничавших на конфиденциальной основе с органами, осуществляющими разведывательную, контрразведывательную и оперативно-разыскную 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, о разработке, об 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 о 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, раскрывающие мероприятия, проводимые в целях обеспечения безопасности государства;

– о мерах по обеспечению защищенности критически важных объектов и потенциально опасных объектов инфраструктуры Российской Федерации от террористических актов;

– о результатах финансового мониторинга в отношении организаций и физических лиц, полученных в связи с проверкой их возможной причастности к террористической деятельности;

– о мерах по обеспечению безопасности критической информационной инфраструктуры Российской Федерации и о состоянии ее защищенности от компьютерных атак.

Принципы отнесения сведений к государственной тайне и засекречивания этих сведений сводится к введению в предусмотренном Законом порядке для сведений, составляющих государственную тайну, ограничений на их распространение и на доступ к их носителям.

Отнесение сведений к государственной тайне и их засекречивание осуществляется в соответствии с принципами законности, обоснованности и своевременности.

Законность отнесения сведений к государственной тайне и их засекречивание заключается в соответствии засекречиваемых сведений Перечню сведений, составляющих государственную тайну, и Списку сведений, не подлежащих отнесению к государственной тайне и засекречиванию, а также законодательству Российской Федерации о государственной тайне.

Законность – правильное применение закона и иных нормативных правовых актов, а также соблюдение всеми должностными лицами, гражданами, предприятиями, учреждениями, организациями требований законодательства о государственной тайне и Конституции РФ.

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.

Обоснованность – основания для отнесения сведений к государственной тайне и их засекречивания должны быть убедительными, подтвержденными серьезными доводами и фактами и основываться на необходимости обеспечения безопасности государства и соблюдения прав и свобод человека и гражданина. Такие доводы и факты могут быть получены при установлении путем экспертной оценки целесообразности засекречивания конкретных сведений, вероятных экономических и иных последствий (например, политических, военных, правоохранительных) этого акта, исходя из баланса жизненно важных интересов государства, общества и граждан. Экспертная оценка заключается в проведении специалистами в соответствующей области определенных исследований, анализа ценности сведений и возможных последствий их преждевременного разглашения для государства, общества и граждан. В силу требований ст. 11 Закона РФ

от 21.07.1993 № 5485-1 «О государственной тайне» 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 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).

Своевременность отнесения сведений к государственной тайне и их засекречивание заключается в установлении ограничений на распространение этих сведений с момента их получения (разработки) или заблаговременно.

Своевременность – отнесение сведений к государственной тайне и их засекречивание должно быть произведено незамедлительно, при получении сведений, разглашение которых может угрожать безопасности государства, либо соответствующие ограничения должны устанавливаться заблаговременно. Например, при проведении научных исследований, опытов в той или иной области науки, при наличии данных, что результаты, которые могут быть получены, подлежат отнесению к государственной тайне, возможные последствия научных изысканий могут быть заранее засекречены.

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 решения 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»** (рис. 2.8).

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.

Рис. 2.8. Грифы секретности информации

Правила отнесения сведений, составляющих государственную тайну, к различным степеням секретности определены Постановлением Правительства Российской Федерации от 4.09.1995 № 870.

Степень секретности сведений, составляющих государственную тайну, должна соответствовать степени тяжести ущерба, который может быть нанесен безопасности Российской Федерации вследствие распространения указанных сведений.

К сведениям особой важности следует относить сведения в области военной, внешнеполитической, экономической, научно-технической, разведывательной, контрразведывательной и оперативно-разыскной деятельности, распространение которых может нанести ущерб интересам Российской Федерации в одной или нескольких из перечисленных областей.

К совершенно секретным сведениям следует относить сведения в области военной, внешнеполитической, экономической, научно-технической, разведывательной, контрразведывательной и оперативно-разыскной деятельности, распространение которых может нанести ущерб интересам министерства (ведомства) или отрасли экономики Российской Федерации в одной или нескольких из перечисленных областей.

К секретным сведениям следует относить все иные сведения из числа сведений, составляющих государственную тайну. Ущербом безопасности Российской Федерации в этом случае считается ущерб, нанесенный интересам предприятия, учреждения или организации в военной, внешнеполитической, экономической, научно-технической, разведывательной, контрразведывательной или оперативно-разыскной области деятельности.

На носители сведений, составляющих государственную тайну, наносятся *реквизиты* (*реквизит* от лат. requisitum – необходимое) – это обязательные сведения, которые должны содержать акт, документ (договор, контракт, вексель, чек и т. п.), чтобы обладать подлинной юридической силой, включающие следующие данные:

– о степени секретности содержащихся в носителе сведений (со ссылкой на соответствующий пункт действующего в данном органе государственной власти, на данном предприятии, в данных учреждении и организации перечня сведений), подлежащих засекречиванию;

– органе государственной власти, о предприятии, об учреждении, организации, осуществивших засекречивание носителя;

– регистрационном номере;

– дате или условии рассекречивания сведений либо о событии, после наступления которого сведения будут рассекречены.

При невозможности нанесения таких реквизитов на носитель сведений, составляющих государственную тайну, эти данные указываются в сопроводительной документации на этот носитель.

Если носитель содержит составные части с различными степенями секретности, каждой из этих составных частей присваивается соответствующий гриф секретности, а носителю в целом присваивается гриф секретности, соответствующий тому грифу секретности, который присваивается его составной части, имеющей высшую для данного носителя степень секретности сведений.

Помимо перечисленных в настоящей статье реквизитов на носителе и (или) в сопроводительной документации к нему могут проставляться дополнительные отметки, определяющие полномочия должностных лиц по ознакомлению с содержащимися в этом носителе сведениями. Вид и порядок проставления дополнительных отметок и других реквизитов определяются нормативными документами, утверждаемыми Правительством Российской Федерации.

2.4. Распоряжение сведениями, составляющими государственную тайну

Как мы можем требовать, чтобы кто-то сохранил нашу тайну,
если мы сами не можем её сохранить?

Ларошфуко

Передача сведений, составляющих государственную тайну, осуществляется:

1. 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.

2. Предприятиями, учреждениями, организациями или гражданами, 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, составляющих государственную тайну, 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.

В договоре на проведение совместных и других работ, заключаемом в установленном законом порядке, предусматриваются

взаимные обязательства сторон по обеспечению сохранности сведений, составляющих государственную тайну, как в процессе проведения работ, так и по их завершении, а также условия финансирования работ (услуг) по защите 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.

При нарушении исполнителем в ходе совместных и других работ, взятых на себя обязательств по защите государственной тайны заказчик вправе приостановить выполнение заказа до устранения нарушений, а при повторных нарушениях – поставить вопрос об аннулировании заказа и лицензии на проведение работ с использованием сведений, составляющих государственную тайну, и о привлечении виновных лиц к ответственности. При этом материальный ущерб, нанесенный исполнителем государству в лице заказчика, подлежит взысканию в соответствии с действующим законодательством.

Обязательным условием для передачи сведений, составляющих государственную тайну, органам государственной власти, предприятиям, учреждениям и организациям является наличие Лицензии (разрешения) на проведение работ с использованием сведений, составляющих государственную тайну, а также выполнение требований нормативных документов, утверждаемых Правительством Российской Федерации, по обеспечению защиты сведений, составляющих государственную тайну, в процессе выполнения работ, связанных с использованием указанных сведений; наличие в их структуре подразделений по защите государственной тайны и специально подготовленных сотрудников для работы по защите информации, количество и уровень квалификации которых достаточны для обеспечения защиты государственной тайны; наличие у них сертифицированных средств защиты информации.

Условия, обеспечивающие защиту передаваемых сведений, должны создаваться начиная с самого момента их передачи.

Так, ч. 5 ст. 22 Федерального закона от 17.07.1999 № 176-ФЗ «О почтовой связи» запрещает прием почтовыми службами от юридических лиц, осуществляющих деятельность в пределах, установленных законодательством Российской Федерации полномочий, почтовых отправлений, содержащих относящиеся к государственной тайне сведения и предметы. Их перевозка и доставка осуществляются силами и средствами специальной связи федерального органа исполнительной власти, осуществляющего управление деятельностью в области связи.

Принимать доставленные в соответствующую организацию сведения, составляющие государственную тайну, и работать с ними должны только лица, имеющие соответствующий допуск к ним, полученный в соответствии с требованиями ст. 21 Закона РФ от 21.07.1993 № 5485-1 «О государственной тайне».

В самой организации, принимающей запрашиваемые секретные сведения, должны быть обеспечены надлежащие условия для их сохранности. Эта организация (предприятие, учреждение, орган власти) должна обладать соответствующим допуском к работе с данными сведениями.

Предусмотренная ст. 16 Закона РФ от 21.07.1993 № 5485-1 «О государственной тайне» ответственность руководителей органов государственной власти, предприятия, учреждения и организации, запрашивающих сведения, за несоблюдение установленных ограничений по ознакомлению со сведениями, составляющими государственную тайну, может быть дисциплинарной, административной или уголовной.

Ст. 17 Закона «О государственной тайне» регулирует вопросы передачи сведений, составляющих государственную тайну, предприятиям, учреждениям, организациям или гражданам в связи с выполнением совместных и других работ. Передача таких сведений 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, если перед передачей сведений, составляющих государственную тайну, в порядке ст. 16 Закона «О государственной

тайне» обязанность проверки наличия у предприятия, учреждения или организации лицензии на проведение работ с использованием сведений соответствующей степени секретности, а у граждан соответствующего допуска лежит на стороне, которая передает такие сведения, и на должностном лице, санкционирующем их передачу, то при передаче сведений, составляющих государственную тайну, предприятиям, учреждениям, организациям или гражданам в связи с выполнением совместных и других работ такую обязанность несет заказчик этих работ.

Правовым основанием для выполнения совместных и других работ служит наличие договора о проведении таких работ между заказчиком и исполнителем. Договор может быть, например, заключен по результатам конкурса на размещение заказа на выполнение работ, либо договор заключается посредством направления оферты (предложения заключить договор) одной из сторон и ее акцепта (принятия предложения) другой стороной.

Государственный контракт на выполнение работ заключается в порядке, предусмотренном ст. 528, 765 и 769-771 ГК РФ.

Особенностью договора на проведение совместных и других работ, связанных с использованием сведений, составляющих государственную тайну, является наличие такого существенного условия, как взаимные обязательства сторон по обеспечению сохранности сведений, составляющих государственную тайну, как в процессе проведения работ, так и по их завершении, а также условия финансирования работ (услуг) по защите сведений, составляющих государственную тайну. Указанные условия считаются существенными, поскольку они названы в законе как существенные или необходимые для договоров данного вида.

Согласно ст. 432 ГК РФ договор считается заключенным, если между сторонами в требуемой форме достигнуто соглашение по всем существенным условиям договора. При отсутствии этих существенных условий договор считается недействительным, поскольку, согласно ст. 168 ГК РФ, сделка, не соответствующая требованиям закона или иных правовых актов, ничтожна. Если договор не предусматривает условий о взаимных обязательствах

сторон по обеспечению сохранности сведений, составляющих государственную тайну, как в процессе проведения работ, так и по их завершении, а также условия финансирования работ (услуг) по защите сведений, составляющих государственную тайну, то такой договор не порождает никаких юридических прав и обязанностей сторон. При этом заказчик не имеет права передавать секретные сведения исполнителю. А орган государственной власти, в распоряжении которого находятся эти сведения, не имеет права давать разрешения на их передачу.

Поскольку заказчик является инициатором заключения договора выполнения работ, именно на заказчике перед заключением договора с исполнителем и передачей ему сведений, составляющих государственную тайну, лежит обязанность проверки наличия у исполнителя лицензии на проведение работ с использованием секретных сведений. Закон возложил организацию контроля за эффективностью защиты государственной тайны при проведении совместных и других работ на заказчика этих работ в соответствии с положениями заключенного сторонами договора.

На исполнителе лежит обязанность выполнить порученные работы с надлежащим качеством и в срок, предусмотренный договором. При этом он должен обеспечить соответствующую защиту секретных сведений, переданных ему для выполнения работ.

Заказчик должен проконтролировать надлежащее качество выполняемых работ, соблюдение сроков их выполнения и своевременно принять результаты выполненных работ и оплатить их.

Ст. 17 Закона «О государственной тайне» предусматривает последствия, которые могут наступить для исполнителя в случае нарушения исполнителем в ходе совместных и других работ, взятых на себя обязательств по защите государственной тайны. А именно: заказчик вправе приостановить выполнение заказа до устранения нарушений, а при повторных нарушениях – поставить вопрос об аннулировании заказа и лицензии на проведение работ с использованием сведений, составляющих государственную тайну, и о привлечении виновных лиц к ответственности.

Согласно ч. 2 и 3 ст. 450 ГК РФ по требованию одной из сторон договор может быть изменен или расторгнут по решению суда только:

– при существенном нарушении договора другой стороной;

– в иных случаях, предусмотренных ГК РФ, другими законами или договором.

Существенным признается нарушение договора одной из сторон, которое влечет для другой стороны такой ущерб, что она в значительной степени лишается того, на что была вправе рассчитывать при заключении договора.

В нашем случае несоблюдение требований о защите секретных сведений является существенным нарушением договора, поскольку его заключение стало возможным только при условии исполнения сторонами взаимных обязательств по защите государственной тайны. При заключении договора заказчик при таких обстоятельствах вправе был рассчитывать на выполнение исполнителем обязательств по защите информации, содержащей государственную тайну, и тем самым обеспечение требований соблюдения принципа недопущения угрозы безопасности государства.

Аннулировать лицензию исполнителя на проведение работ с использованием секретных сведений может орган, ее выдавший, по представлению заказчика.

При этом материальный ущерб, нанесенный исполнителем государству в лице заказчика, подлежит взысканию в соответствии с действующим законодательством.

Материальный ущерб может выразиться:

– в затратах на устранение последствий несоблюдения требований о защите секретных сведений (например, на розыск и поимку лиц, неправомерно завладевших в результате халатности исполнителя секретной информацией);

– в утрате или использовании исполнителем переданных ему заказчиком товарно-материальных ценностей для исполнения договора выполнения работ;

– понесенных затратах на устройство нового конкурса по размещению невыполненного государственного заказа и т. д.

Материальный ущерб, нанесенный исполнителем государству в лице заказчика, взыскивается путем предъявления иска в соответствующий суд с приложением расчета причиненного ущерба, договора о выполнении работ и документов, подтверждающих обстоятельства дела.

В соответствии со ст. 18 Закона «О государственной тайне» передачей сведений другим государствам является доведение до иностранного государства (уполномоченного государством представителя) каким-либо способом (передача, пересылка, ознакомление, осуществление доступа) указанных сведений.

Необходимым условием для передачи этих сведений является наличие положительного экспертного заключения межведомственной комиссии по защите государственной тайны о возможности передачи.

Передача сведений, составляющих государственную тайну, другим государствам осуществляется, как правило, в соответствии с международным договором (соглашением), заключенным с этими государствами по предмету обмена и защиты секретных сведений.

Согласно требованиям Положения о подготовке к передаче сведений, составляющих государственную тайну, другим государствам (утвержденного Постановлением Правительства РФ от 02.08.1997 № 973) обязательства принимающей стороны (иностранного государства) по защите передаваемых ей сведений предусматриваются в заключаемом с ней международном договоре, разделы (статьи, пункты) которого должны содержать:

– соотнесение степеней секретности передаваемых сведений в Российской Федерации и в иностранном государстве;

– перечень компетентных органов, уполномоченных осуществлять прием (передачу) сведений и несущих ответственность за их защиту;

– порядок передачи сведений;

– требования к использованию и обработке передаваемых сведений;

– обязательства о нераспространении передаваемых сведений третьим странам и их защите в соответствии с внутренним законодательством принимающей стороны;

– порядок разрешения конфликтных ситуаций и возмещения возможного ущерба.

В соответствии с порядком передачи секретных сведений иностранным государством, установленном в РФ, заинтересованные в передаче сведений федеральные органы исполнительной власти, органы исполнительной власти субъектов Российской Федерации, предприятия, учреждения и организации направляют руководителям органов государственной власти РФ, наделенным полномочиями по распоряжению сведениями, мотивированное ходатайство, в котором излагаются:

– цель передачи;

– перечень планируемых к передаче сведений, их степень секретности, кем и на каком основании они были засекречены (отнесены к государственной тайне);

– перечень компетентных органов, уполномоченных принимающей стороной получать сведения;

– обоснование необходимости и целесообразности передачи сведений, оценка последствий такой передачи для обеспечения политических и экономических интересов Российской Федерации;

– предполагаемый порядок возмещения ущерба в случае невыполнения принимающей стороной взятых на себя обязательств.

Получивший мотивированное ходатайство орган государственной власти изучает возможность передачи запрашиваемых сведений и в месячный срок доводит свое решение до заявителя.

Мотивированное ходатайство, решение органов государственной власти, руководители которых наделены полномочиями по распоряжению сведениями, а также международные договоры и другие документы, имеющие непосредственное отношение к защите рассматриваемых к передаче сведений, заявитель представляет в Межведомственную комиссию для подготовки экспертного заключения.

Экспертное заключение Межведомственной комиссии, содержащее вывод о возможности передачи сведений с учетом соблюдения интересов Российской Федерации, направляется заявителю в сорокапятидневный срок с момента получения материалов. В случае

необходимости проведения дополнительной экспертизы срок подготовки экспертного заключения может быть увеличен, о чем сообщается заявителю.

Затем федеральными органами исполнительной власти, руководители которых наделены полномочиями по распоряжению сведениями, органами исполнительной власти субъектов Российской Федерации по ходатайству организации-заявителя проект решения Правительства Российской Федерации с экспертным заключением Межведомственной комиссии вносится в установленном порядке в Правительство Российской Федерации.

В случае если с иностранным государством – получателем сведений, ранее не заключался международный договор о взаимном обеспечении защиты передаваемых сведений или при неполном отражении в заключенном ранее международном договоре правил, изложенных в Положении о подготовке к передаче сведений, составляющих государственную тайну, другим государствам, одновременно с проектом решения о передаче сведений в Правительство Российской Федерации представляются предварительно проработанные с принимающей стороной согласованные с заинтересованными федеральными органами исполнительной власти предложения о заключении соответствующего международного договора или дополнении действующего.

На основании решения Правительства Российской Федерации в соответствии с процедурами, предусмотренными международным договором и действующими нормативными правовыми актами, принимаемыми по каждому факту передачи секретных сведений отдельно, осуществляется фактическая передача сведений.

Дополнительные меры защиты передаваемых сведений могут быть предусмотрены в соглашениях или контрактах, заключаемых (подписываемых) компетентными органами, уполномоченными осуществлять прием (передачу) сведений.

Руководители федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации, предприятий, учреждений и организаций, уполномоченных Правительством Российской Федерации осуществлять передачу

сведений другим государствам, несут ответственность за нарушение или ненадлежащее исполнение Положения в соответствии с законодательством Российской Федерации. Ответственностью для юридического лица может являться лишение допуска к проведению работ с использованием сведений, составляющих государственную тайну, и наложение обязанности возместить ущерб, причиненный за нарушение правил приема, передачи секретных сведений.

На практике предусматриваются случаи, когда органы государственной власти, предприятия, учреждения и организации, располагающие сведениями, составляющими государственную тайну, *теряют право на обладание сведениями, составляющими государственную тайну*, и их носителями при изменении их функций, форм собственности, ликвидации или прекращения работ с использованием сведений, составляющих государственную тайну.

Изменение формы собственности может произойти в результате приватизации или продажи юридического лица.

Прекращение работ с использованием сведений, составляющих государственную тайну, может произойти в связи с выполнением условий государственного контракта на проведение этих работ и отсутствия какого-либо нового аналогичного контракта.

Закон «О государственной тайне» возлагает на органы государственной власти, предприятия, учреждения и организации, располагающие сведениями, составляющими государственную тайну, и потерявшими право на обладание этими сведениями, обязанность принять меры по обеспечению защиты этих сведений и их носителей с тем, чтобы не допустить возникновения угрозы безопасности государства.

При этом носители сведений, составляющих государственную тайну, в установленном порядке уничтожаются, сдаются на архивное хранение либо передаются правопреемнику органа государственной власти, предприятия, учреждения или организации, располагающих сведениями, составляющими государственную тайну, если этот правопреемник имеет полномочия по проведению работ с использованием указанных сведений.

Если же правопреемника не существует либо он не обладает полномочиями по проведению работ с использованием секретных сведений и в иных случаях, предусмотренных данной статьей, носители сведений, составляющих государственную тайну, сдаются на архивное хранение либо передаются:

– органу государственной власти, в распоряжении которого в соответствии со ст. 9 Закона «О государственной тайне» находятся сведения, составляющие государственную тайну (в случаях, когда по решению этого органа власти секретные сведения ранее передавались государственному органу или юридическому лицу, от которого они поступают в обратном порядке);

– другому органу государственной власти, предприятию, учреждению или организации по указанию Межведомственной комиссии по защите государственной тайны.

Порядок уничтожения секретных документов разрабатывается каждым министерством или ведомством, чьи руководители обладают полномочиями по отнесению сведений к государственной тайне отдельно, согласно рекомендациям Межведомственной комиссии по защите государственной тайны.

Защита сведений, составляющих государственную тайну, при изменении функций субъектов правоотношений.

Органы государственной власти, предприятия, учреждения и организации, располагающие сведениями, составляющими государственную тайну, в случаях изменения их функций, форм собственности, ликвидации или прекращения работ с использованием сведений, составляющих государственную тайну, обязаны принять меры по обеспечению защиты этих сведений и их носителей. При этом носители сведений, составляющих государственную тайну, в установленном порядке уничтожаются, сдаются на архивное хранение либо передаются:

– правопреемнику органа государственной власти, предприятия, учреждения или организации, располагающих сведениями, составляющими государственную тайну, если этот правопреемник имеет полномочия по проведению работ с использованием указанных сведений;

– органу государственной власти, в распоряжении которого находятся соответствующие сведения;

– другому органу государственной власти, предприятию, учреждению или организации по указанию межведомственной комиссии по защите государственной тайны.

2.5. Допуск должностных лиц и граждан к государственной тайне

Должно хранить тайны своих друзей. Не хранящий тайну бесчестит свою совесть и посрамляет доверие к себе.

Иоанн Дамаскин

Законодательством Российской Федерации закреплен принцип добровольности допуска граждан к государственной тайне. Однако этот принцип относительно декларативен, поскольку, если должность, на которую претендует лицо, связана с необходимостью работы с секретными сведениями, а у лица отсутствует допуск к ним, назначение на эту должность возможно только после оформления допуска к сведениям, составляющим государственную тайну.

Основополагающие принципы по порядку допуска должностных лиц и граждан к государственной тайне определены в Законе Российской Федерации от 21.07.1993 № 5485-1 «О государственной тайне» и развиты в Постановлении Правительства Российской Федерации от 06.02.2010 № 63 «Об утверждении Инструкции о порядке допуска должностных лиц и граждан Российской Федерации к государственной тайне».

Допуск к государственной тайне, оформленный до вступления в силу данного Постановления, действителен до окончания срока действия допуска.

Федеральной службе безопасности Российской Федерации предоставлено право давать государственным органам, органам местного самоуправления и организациям разъяснения по вопросам применения Инструкции, утвержденной данным Постановлением.

В Инструкции используются следующие *основные понятия*:

– «доступ к сведениям, составляющим государственную тайну» – санкционированное полномочным должностным лицом ознакомление конкретного работника со сведениями, составляющими государственную тайну;

– «близкие родственники» – жена (муж), отец, мать, дети, усыновители, усыновленные, полнородные и неполнородные (имеющие общих отца или мать) братья и сестры;

– «постоянное проживание за границей» – проживание граждан за пределами Российской Федерации более шести месяцев в течение года, не связанное с исполнением ими обязанностей государственной службы;

– «номер допуска к государственной тайне» – номер отметки о проведении проверочных мероприятий, проставляемый органами безопасности, а при оформлении допуска к государственной тайне без проведения органами безопасности проверочных мероприятий – номер соответствующего удостоверения либо учетный номер карточки (форма 1).

В соответствии со степенями секретности сведений, составляющих государственную тайну, устанавливаются следующие *формы допуска граждан к государственной тайне*:

– первая форма – для граждан, допускаемых к сведениям особой важности;

– вторая форма – для граждан, допускаемых к совершенно секретным сведениям;

– третья форма – для граждан, допускаемых к секретным сведениям.

Доступ граждан к сведениям, составляющим государственную тайну, разрешается только при наличии у них допуска к государственной тайне по соответствующей форме. Наличие у граждан допуска к сведениям более высокой степени секретности является основанием для их доступа к сведениям более низкой степени секретности.

Оформление гражданам допуска к государственной тайне осуществляется по месту работы (службы) (рис. 2.9).

Рис. 2.9. Формы допуска

Если по характеру выполняемых должностных (специальных, функциональных) обязанностей предусматривается доступ к сведениям, составляющим государственную тайну, граждане могут быть назначены на эти должности только после оформления допуска к государственной тайне по соответствующей форме.

Лица, имеющие двойное гражданство, допускаются к сведениям, составляющим государственную тайну, только с грифом «секретно» и после проведения проверочных мероприятий органами федеральной службы безопасности.

Лица без гражданства могут быть допущены к сведениям, составляющим государственную тайну, на основании решения Правительства Российской Федерации. При этом к сведениям особой важности и совершенно секретным сведениям лица без гражданства, как правило, не допускаются.

Иностранные граждане допускаются к государственной тайне на основании международного договора, предусматривающего обязательства иностранного государства по защите передаваемых ему сведений, составляющих государственную тайну.

Решение о допуске иностранных граждан к государственной тайне принимается руководителями органов государственной власти Российской Федерации, органов государственной власти субъектов Российской Федерации, предприятий, учреждений, организаций, уполномоченных Правительством Российской Федерации осуществлять передачу сведений, составляющих

государственную тайну, другому государству. Указанное решение согласовываетсяс Федеральной службой безопасности Российской Федерации.

Допуск граждан к государственной тайне предусматривает:

а) принятие на себя обязательств перед государством по нераспространению доверенных им сведений, составляющих государственную тайну;

б) письменное согласие на частичные, временные ограничения их прав в соответствии со ст. 24 Закона Российской Федерации «О государственной тайне»;

в) письменное согласие на проведение в отношении их полномочными органами проверочных мероприятий;

г) определение видов, размеров и порядка предоставления социальных гарантий, предусмотренных законодательством Российской Федерации;

д) ознакомление с нормами законодательства Российской Федерации о государственной тайне, предусматривающими ответственность за его нарушение;

е) принятие руководителем организации решения (в письменном виде) о допуске оформляемого гражданина к сведениям, составляющим государственную тайну.

Проверочные мероприятия, связанные с оформлением допуска граждан к государственной тайне, осуществляются органами безопасности по месту расположения организаций, их территориально обособленных подразделений.

Проверочные мероприятия, связанные с оформлением допуска к государственной тайне сотрудников и граждан, принимаемых на службу (работу) в федеральный орган исполнительной власти, уполномоченный в области внешней разведки, осуществляются указанным федеральным органом исполнительной власти во взаимодействии с федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности.

При этом проверочные мероприятия могут проводиться как при получении первичного допуска к государственной тайне, так и повторно. Необходимость в проведении повторных проверочных

мероприятий может возникнуть при переоформлении допуска к государственной тайне, в случае оформления допуска по более высокой степени секретности.

Согласно ч. 3 ст. 21 Закона Российской Федерации «О государственной тайне» допуск должностных лиц и граждан к государственной тайне предусматривает частичные временные ограничения их прав в соответствии со ст. 24 названного Закона, которой установлено в том числе ограничение прав на неприкосновенность частной жизни при проведении проверочных мероприятий в период оформления допуска к государственной тайне.

Уклонение от проверочных мероприятий или сообщение заведомо ложных анкетных данных в соответствии с ч. 1 ст. 22 и ч. 1 ст. 23 того же закона являются одним из оснований для отказа должностному лицу или гражданину в допуске к государственной тайне либо к прекращению такого допуска.

Следует учитывать, что основаниями для отказа в допуске к государственной тайне могут появиться уже после того, как лицо получило такой допуск. Ст. 22 Закона «О государственной тайне» предусматривает возникновение вышеперечисленных обстоятельств в качестве условий прекращения допуска к государственной тайне.

В связи с этим, как представляется, проведение проверочных мероприятий не может ограничиваться периодом оформления допуска к государственной тайне. Проверочные мероприятия должны проводиться по мере необходимости и после получения такого допуска, чтобы обеспечивать своевременное получение сведений о возможном возникновении обстоятельств, являющихся основанием для отказа в допуске к государственной тайне, прекращения допуска к государственной тайне.

Проведение проверочных мероприятий регламентируется Федеральным законом «Об оперативно-разыскной деятельности».

Так, согласно п. 1 ч. 2 ст. 7 Закона об ОРД, органы, осуществляющие оперативно-розыскную деятельность, в пределах своих полномочий вправе собирать данные, необходимые для принятия решений о допуске к сведениям, составляющим государственную

тайну. В то же время, в соответствии с ч. 7 ст. 8 Закона об ОРД, устанавливаются ограничения для проведения оперативно-разыскных мероприятий, осуществляемых по данному основанию, а именно – запрещается использование мероприятий, указанных в пунктах 8–11 ч. 1 ст. 6 этого закона: обследования помещений, зданий, сооружений, участков местности и транспортных средств (п. 8), контроля почтовых отправлений, телеграфных и иных сообщений (п. 9), прослушивания телефонных переговоров (п. 10) и снятие информации с технических каналов связи (п. 11).

В ходе проведения оперативно-разыскных мероприятий, как это оговорено в ч. 3 ст. 6 Закона об ОРД, допускается использование информационных систем, видео- и аудиозаписи, кино- и фотосъемки, а также других технических и иных средств, не наносящих ущерб жизни и здоровью.

Гражданство, национальность, пол, место жительства, имущественное, должностное и социальное положение, принадлежность к общественным объединениям, отношение к религии и политические убеждения отдельных лиц не являются препятствием для проведения в отношении них оперативно-разыскных мероприятий на территории Российской Федерации, если иное не предусмотрено Федеральным законом.

С учетом результатов проверочных мероприятий в индивидуальном порядке принимается решение по конкретному лицу о допуске или об отказе в допуске к государственной тайне. В частности, основанием для отказа гражданину в допуске к государственной тайне в соответствии со ст. 22 Закона Российской Федерации «О государственной тайне» могут являться выявления в результате проведения проверочных мероприятий действий оформляемого лица, создающих угрозу безопасности Российской Федерации.

Допуск граждан к государственной тайне по третьей форме оформляется без проведения органами безопасности проверочных мероприятий. В случае если имеются сомнения в достоверности предоставленных гражданами анкетных данных, руководитель организации может в установленном порядке направить

материалы в орган безопасности для проведения проверочных мероприятий.

Руководителям организаций, работникам их структурных подразделений по защите государственной тайны, а также лицам, на которых возлагается исполнение функций структурных подразделений по защите государственной тайны, допуск к государственной тайне оформляется с проведением органами безопасности проверочных мероприятий.

Органы безопасности по согласованию с заинтересованными организациями определяют организации, в которых допуск к государственной тайне по третьей форме оформляется с проведением органами безопасности проверочных мероприятий.

Обязательства граждан перед государством по соблюдению требований законодательства Российской Федерации о государственной тайне, с которыми заключается трудовой договор (контракт), отражаются в трудовом договоре (контракте), а обязательства граждан, с которыми не заключается трудовой договор (контракт), оформляются в виде расписки.

Члены Совета Федерации Федерального Собрания Российской Федерации, депутаты Государственной Думы Федерального Собрания Российской Федерации, судьи на период исполнения ими своих полномочий, а также адвокаты, участвующие в качестве защитников в уголовном судопроизводстве по делам, связанным со сведениями, составляющими государственную тайну, допускаются к сведениям, составляющим государственную тайну, без проведения проверочных мероприятий, предусмотренных ст. 21 Закона Российской Федерации «О государственной тайне».

Указанные лица предупреждаются о неразглашении государственной тайны, ставшей им 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.

Основаниями для отказа гражданину в допуске к государственной тайне могут являться:

а) признание гражданина недееспособным или ограниченно дееспособным на основании решения суда, вступившего в законную

силу, наличие у него статуса обвиняемого (подсудимого) по уголовному делу о совершенном по неосторожности преступлении против государственной власти или об умышленном преступлении, наличие у него непогашенной или неснятой судимости за данные преступления, прекращение в отношении его уголовного дела (уголовного преследования) по нереабилитирующим основаниям, если со дня прекращения такого уголовного дела (уголовного преследования) не истек срок, равный сроку давности привлечения к уголовной ответственности за совершение этих преступлений;

б) наличие у гражданина медицинских противопоказаний для работы с использованием сведений, составляющих государственную тайну, согласно перечню, утверждаемому федеральным органом исполнительной власти, уполномоченным в области здравоохранения и социального развития;

в) постоянное проживание его самого и (или) его близких родственников за границей и (или) оформление указанными гражданами документов для выезда на постоянное место жительства в другие государства;

г) выявление в результате проведения проверочных мероприятий действий гражданина, создающих угрозу безопасности Российской Федерации;

д) уклонение гражданина от проверочных мероприятий и (или) сообщение заведомо ложных анкетных данных.

Решение о допуске к государственной тайне принимается:

а) в отношении граждан, пребывающих в запасе и подлежащих призыву на военную службу по мобилизации или на военные сборы, – военным комиссаром;

б) в отношении руководителей государственных органов и государственных организаций – теми, кем они были назначены на соответствующие должности;

в) в отношении руководителей негосударственных организаций – руководителем организации – заказчика работ с использованием сведений, составляющих государственную тайну.

Оформление допуска к государственной тайне руководителям государственных органов и государственных организаций, а также

руководителям негосударственных организаций осуществляется организацией, должностное лицо которой принимает решение о допуске к государственной тайне. В организацию, руководителю которой оформлен допуск к государственной тайне, направляется письмо, заверенное печатью организации (при наличии печати), оформлявшей допуск к государственной тайне, в котором указываются дата окончания проверочных мероприятий, форма и номер допуска к государственной тайне, наименование органа безопасности, проводившего проверочные мероприятия, и дата принятия решения о допуске к государственной тайне.

Допуск гражданина к государственной тайне может быть прекращен по решению должностного лица, принявшего решение о его допуске к государственной тайне, в случае:

а) расторжения с ним трудового договора (контракта) в связи с проведением организационных и (или) штатных мероприятий;

б) однократного нарушения им обязательств, связанных с защитой государственной тайны;

в) возникновения обстоятельств, являющихся основаниями для отказа гражданину в допуске к государственной тайне.

Решение о прекращении допуска к государственной тайне может быть обжаловано гражданином в вышестоящей организации или в суде.

Прекращение допуска к государственной тайне не освобождает гражданина от ранее взятых им обязательств по неразглашению сведений, составляющих государственную тайну.

Руководители организаций несут персональную ответственность за подбор граждан, допускаемых к государственной тайне.

Перечень должностей, при назначении на которые гражданам оформляется допуск к государственной тайне, определяется номенклатурой должностей работников, подлежащих оформлению на допуск к государственной тайне, разрабатываемой в организации и согласованной с органом безопасности.

Граждане, которым оформляется допуск к государственной тайне, представляют собственноручно заполненную анкету, документы, удостоверяющие личность и подтверждающие сведения,

указанные в анкете (паспорт, военный билет, трудовую книжку, свидетельство о рождении, свидетельство о заключении (расторжении) брака, диплом об образовании и т. п.), а также справку об отсутствии медицинских противопоказаний для работы со сведениями, составляющими государственную тайну. Форму и порядок получения должностными лицами и гражданами Российской Федерации справки об отсутствии медицинских противопоказаний для работы с использованием сведений, составляющих государственную тайну, утверждены Приказом Министерства здравоохранения и социального развития РФ от 26.08.2011 № 989н.

К таким противопоказаниям относят:

– органические, включая симптоматические, психические расстройства;

– шизофрения, шизотипические и бредовые расстройства;

– расстройства настроения (аффективные расстройства);

– расстройства привычек и влечений;

– умственная отсталость;

– психические расстройства и расстройства поведения, связанные с употреблением психоактивных веществ;

– эпилепсия.

Документы для оформления допуска к государственной тайне работнику подготавливают работники кадрового подразделения:

а) знакомят гражданина, оформляемого на допуск к государственной тайне, с нормами законодательства Российской Федерации о государственной тайне, предусматривающими ответственность за его нарушение;

б) сверяют сведения, указанные гражданином в анкете, со сведениями, содержащимися в представленных документах;

в) уточняют при необходимости отдельные сведения, указанные в анкете;

г) доводят до гражданина, оформляемого на допуск к государственной тайне, обязательства перед государством о соблюдении требований законодательства Российской Федерации о государственной тайне.

Анкета гражданина, которому оформляется допуск к государственной тайне, подписывается работником кадрового подразделения и заверяется печатью организации или кадрового подразделения (при наличии печати) и передается в режимно-секретное подразделение, которое в свою очередь:

а) разрабатывает рекомендации для кадрового подразделения по порядку оформления на работу (службу) граждан на должности, предусматривающие работу со сведениями, составляющими государственную тайну;

б) запрашивает карточки (форма 1) в режимно-секретных подразделениях тех организаций, в которых оформляемые на работу (службу) граждане работали (служили) в течение последних 5 лет;

в) анализирует материалы, представляемые кадровым подразделением и полученные от режимно-секретных подразделений с прежних мест работы (службы) граждан, оформляемых на работу (службу), на предмет выявления наличия возможных оснований для отказа гражданину в оформлении допуска к государственной тайне;

г) оформляет, учитывает и хранит карточки (форма 1), копии трудового договора (контракта) и расписки, содержащие обязательства граждан по соблюдению требований законодательства Российской Федерации о государственной тайне (форма 2);

д) осуществляет контроль за исполнением установленных требований по допуску граждан к государственной тайне;

е) осуществляет учет предписаний на выполнение задания (форма 5) и справок о соответствующей форме допуска (формы 6–8);

ж) проводит инструктаж граждан, допускаемых к государственной тайне.

з) направляет в орган безопасности следующие документы для оформления допуска к государственной тайне в соответствии с Инструкцией о порядке допуска должностных лиц и граждан Российской Федерации к государственной тайне.

и) хранит карточки о допуске вместе с копиями трудового договора (контракта) или расписками, содержащими обязательства граждан по соблюдению требований законодательства Российской Федерации о государственной тайне.

В случае отсутствия в организации режимно-секретного подразделения или работника, исполняющего функции режимно-секретного подразделения, оформление допусков к государственной тайне осуществляется режимно-секретным подразделением организации, которая оказывает данной организации услуги по защите государственной тайны.

Органы безопасности могут запрашивать в организациях дополнительные документы, необходимые для проведения проверочных мероприятий.

Документы, не соответствующие требованиям настоящей инструкции, возвращаются органом безопасности для доработки.

На гражданина, которому оформляется допуск к государственной тайне, заводится одна карточка. При переходе гражданина на работу (службу) в другую организацию указанная карточка по письменному запросу режимно-секретного подразделения соответствующей организации пересылается по новому месту работы (службы).

Новая карточка заводится только в случае, если ранее заведенная карточка была уничтожена в установленном порядке.

Карточка, оформленная на гражданина, допущенного к государственной тайне по третьей форме без проведения органами безопасности проверочных мероприятий, в другие организации не пересылается.

Если в течение 6 месяцев после проведения проверочных мероприятий не было принято решение о допуске гражданина к государственной тайне, отметка о проведении проверочных мероприятий органами безопасности в карточке (форма 1) становится недействительной.

В этом случае в орган безопасности, проводивший проверочные мероприятия, в месячный срок направляется соответствующее уведомление.

В отношении граждан, которые переведены на должности, не предусматривающие наличие допуска к государственной тайне, уволились из организации, в том числе при расторжении трудового договора (контракта) в связи с проведением организационных и (или) штатных мероприятий, закончили обучение в учебном

заведении и т. п. и на которых в течение шести месяцев не затребованы карточки, действие допуска прекращается.

После прекращения допуска к государственной тайне копия трудового договора (контракта) или расписка, содержащая обязательства гражданина по соблюдению требований законодательства Российской Федерации о государственной тайне, и карточка хранятся в режимно-секретном подразделении до истечения срока наложения ограничений на права гражданина, но не менее 5 лет, после чего уничтожаются в установленном порядке.

Работа по совместительству

При необходимости оформления гражданину, имеющему допуск к государственной тайне, такого же допуска для работы по совместительству в другой организации (в том числе и в качестве арбитражного управляющего) по соответствующему запросу изготавливается установленным порядком дубликат карточки, который направляется в запрашивающую организацию. По этому дубликату принимается решение о допуске к государственной тайне. Если переоформления допуска к государственной тайне не требуется, гражданин в установленном порядке допускается к государственной тайне и назначается на должность, а режимно-секретное подразделение не позднее чем через месяц направляет в орган безопасности уведомление.

Гражданам, допущенным к государственной тайне в организации, в которой они работают по совместительству, запрещается использование сведений, составляющих государственную тайну, полученных в организации по основному месту работы.

Указанные сведения могут быть переданы в организацию, в которой граждане работают по совместительству, в установленном порядке.

Переоформление допуска к государственной тайне

Переоформление допуска к государственной тайне по первой форме производится через десять лет, по второй и третьей (с проведением органами безопасности проверочных мероприятий) формам производится через пятнадцать лет с даты окончания проведения проверочных мероприятий органами безопасности в случае перехода указанных граждан на другое место работы (службы).

Переоформление допуска к государственной тайне граждан, постоянно работающих в организации, оформившей им данный допуск, не производится.

Переоформление допуска к государственной тайне по первой, второй и третьей (с проведением органами безопасности проверочных мероприятий) формам независимо от срока действия производится в следующих случаях:

а) прием гражданина на работу (службу), назначение на должность в структурные подразделения по защите государственной тайны, за исключением случая перевода гражданина из одного структурного подразделения по защите государственной тайны в другое в рамках одной организации;

б) вступление гражданина в брак, кроме случая, предусмотренного п. 63 настоящей инструкции;

в) возвращение из длительной, свыше 6 месяцев, заграничной командировки;

г) возникновение обстоятельств, являющихся основаниями для отказа гражданину в допуске к государственной тайне, влияющие на принятие решения о допуске к государственной тайне;

д) прием на работу (службу) гражданина, который ранее относился к одной из категорий граждан: члены Совета Федерации Федерального Собрания Российской Федерации, депутаты Государственной Думы Федерального Собрания Российской Федерации, судьи на период исполнения ими своих полномочий, а также адвокаты, участвующие в качестве защитников в уголовном судопроизводстве по делам, связанным со сведениями, составляющими государственную тайну, которые были допущены к сведениям, составляющим государственную тайну, без проведения проверочных мероприятий;

е) прием на работу (службу) гражданина, у которого в карточке (форма 1) в позиции 7 проставлена особая отметка органа безопасности;

ж) прием на работу (службу) гражданина, пребывающего в запасе, если с даты принятия военным комиссаром решения о его допуске к государственной тайне прошло более шести месяцев;

з) призыв гражданина, пребывающего в запасе, карточка (форма 1) которого хранится в военном комиссариате, для прохождения плановых военных сборов на воинских должностях, замещение которых предусматривает работу со сведениями, составляющими государственную тайну, если с даты принятия военным комиссаром решения о его допуске к государственной тайне прошло более шести месяцев;

и) прием на работу (службу) гражданина, у которого в карточке (форма 1) в позиции 10 имеется отметка о нарушениях режима секретности и (или) наличии оснований для отказа в допуске к государственной тайне.

Допуск к государственной тайне не переоформляется в следующих случаях:

– вступление гражданина в брак с лицом, имеющим допуск к государственной тайне, оформленный с проведением органами безопасности проверочных мероприятий;

– смена гражданином фамилии, имени или отчества в случаях, предусмотренных законодательством Российской Федерации.

Режимно-секретное подразделение вносит соответствующие изменения в карточку и в месячный срок направляет в орган безопасности соответствующее уведомление.

Кадровое подразделение обязано в десятидневный срок информировать режимно-секретное подразделение обо всех изменениях в биографических данных гражданина, допущенного к государственной тайне, для решения вопроса о целесообразности переоформления ему допуска к государственной тайне и внесения соответствующих изменений в карточку.

Доступ граждан к сведениям, составляющим государственную тайну, в организациях, в которые они командируются

Доступ граждан к сведениям, составляющим государственную тайну, в организациях, в которые они командируются, осуществляется после предъявления ими предписаний на выполнение задания, документов, удостоверяющих личность, и справок о допуске по соответствующей форме.

Сотрудникам органов безопасности, осуществляющим по роду службы взаимодействие с организациями в работе по защите

государственной тайны, право доступа к сведениям, составляющим государственную тайну, предоставляется по предъявлении служебного удостоверения и справок о допуске по соответствующей форме.

Справка о допуске по соответствующей форме подписывается руководителем режимно-секретного подразделения и заверяется печатью организации (при наличии печати). Указанная справка регистрируется в журнале учета выдачи справок о допуске и выдается командируемому на время разовой командировки или на период выполнения задания, но не более чем на год, под расписку. По окончании срока действия справка возвращается по месту ее выдачи, подшивается в отдельное дело и хранится не менее пяти лет. Журнал учета выдачи справок о допуске после его закрытия в установленном порядке хранится в режимно-секретном подразделении не менее пяти лет.

Требовать от командированного гражданина, прибывшего в организацию для выполнения задания, не связанного с работами со сведениями, составляющими государственную тайну, справку о допуске по соответствующей форме запрещается. Исключение составляют случаи, когда командированный гражданин при выполнении задания неизбежно будет иметь доступ к сведениям, составляющим государственную тайну.

Предписание на выполнение задания подписывается руководителем организации, а в органе государственной власти, Государственной корпорации по атомной энергии «Росатом», Государственной корпорации по космической деятельности «Роскосмос» – должностным лицом, уполномоченным, соответственно, руководителем органа государственной власти, Государственной корпорации по атомной энергии «Росатом», Государственной корпорации по космической деятельности «Роскосмос», заверяется печатью, соответственно, организации (при наличии печати), органа государственной власти, указанных государственных корпораций и регистрируется в журнале учета выдачи предписаний на выполнение заданий.

В предписании на выполнение задания указывается основание для командирования (номер и дата постановления, решения,

договора, совместного плана научно-исследовательских и опытно-конструкторских работ и т. п.).

Предписание на выполнение задания, в котором содержатся сведения, составляющие государственную тайну, пересылается в установленном порядке.

Предписание на выполнение задания выдается для посещения только одной организации.

Доступ командированных граждан к сведениям, составляющим государственную тайну, осуществляется по письменному разрешению руководителя принимающей организации, а в органах государственной власти, Государственной корпорации по атомной энергии «Росатом», Государственной корпорации по космической деятельности «Роскосмос» – должностного лица, уполномоченного руководителем, соответственно, органа государственной власти, Государственной корпорации по атомной энергии «Росатом», Государственной корпорации по космической деятельности «Роскосмос». Разрешение оформляется на предписании на выполнение задания с указанием конкретных носителей сведений, составляющих государственную тайну, с которыми можно ознакомить командированного гражданина.

Предписание на выполнение задания и справка о допуске по соответствующей форме регистрируются в журнале учета командированных. После регистрации справка о допуске по соответствующей форме остается в режимно-секретном подразделении принимающей организации, а предписание на выполнение задания с отметкой о форме допуска командированного гражданина передается принимающему его должностному лицу. Указанное должностное лицо заполняет на оборотной стороне предписания на выполнение задания справку, после чего данное предписание передается в режимно-секретное подразделение принимающей организации, где хранится в отдельном деле не менее 5 лет. Справка о допуске по соответствующей форме возвращается командированному гражданину для сдачи в выдавшее ее режимно-секретное подразделение. На обороте справки о допуске по соответствующей форме делается запись с указанием степени секретности сведений, с которыми ознакомился командированный

гражданин, и даты ознакомления, которая заверяется подписью руководителя режимно-секретного подразделения принимающей организации и печатью этой организации (при наличии печати).

Указанные в справке о допуске по соответствующей форме данные об ознакомлении гражданина со сведениями, составляющими государственную тайну, переносятся в карточку учета осведомленности в сведениях, составляющих государственную тайну.

Социальные гарантии гражданам, допущенным к государственной тайне на постоянной основе, и сотрудникам структурных подразделений по защите государственной тайны

В соответствии с со ст. 21 Закона Российской Федерации «О государственной тайне» 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, установленным для должностных лиц и граждан, допущенных к государственной тайне на постоянной основе, устанавливается процентная надбавка к заработной плате за стаж работы в указанных структурных подразделениях.

Определение видов, размеров и порядка предоставления социальных гарантий, предусмотренных настоящим Законом «О государственной тайне» и Постановлением Правительства РФ от 18.09.2006 № 573.

Ежемесячная процентная надбавка к должностному окладу (тарифной ставке) граждан, допущенных к государственной тайне на постоянной основе (за исключением военнослужащих, сотрудников органов внутренних дел Российской Федерации и уголовно-исполнительной системы), выплачивается в зависимости

Рис. 2.10. Размер ежемесячной процентной надбавки за работу со сведениями, составляющими государственную тайну

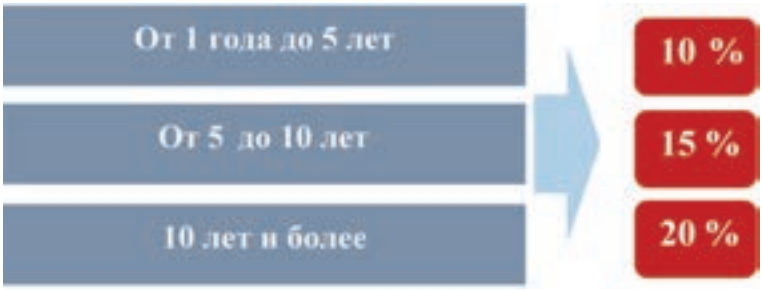

Рис. 2.11. Размер ежемесячной процентной надбавки за стаж работы в структурных подразделениях по защите государственной тайны

от степени секретности сведений, к которым эти граждане имеют документально подтверждаемый доступ на законных основаниях (рис. 2.10, 2.11).

В стаж работы сотрудников структурных подразделений по защите государственной тайны, дающий право на получение надбавки, включается время работы в структурных подразделениях по защите государственной тайны других органов государственной власти, органов местного самоуправления и организаций (в соответствии с Приказом Министерства здравоохранения и социального развития РФ от 19 мая 2011 г. № 408н «О порядке

выплаты ежемесячных процентных надбавок гражданам, допущенным к государственной тайне на постоянной основе, и сотрудникам структурных подразделений по защите государственной тайны»).

Под постоянной работой со сведениями, составляющими государственную тайну, следует понимать работу с этими сведениями независимо от порядка и условий их получения (в виде письменного документа, при использовании технических средств, в процессе обучения и др.), а также независимо от продолжительности работы и ее периодичности в течение года.

Выплата процентных надбавок за работу со сведениями, составляющими государственную тайну, производится с момента письменного оформления соответствующего решения (приказа, распоряжения, указания) руководителя (командира) государственного органа, органа местного самоуправления, организации, воинской части (далее – приказ (распоряжение, указание)) о работе гражданина на постоянной основе со сведениями, составляющими государственную тайну, соответствующей степени секретности в соответствии с должностными регламентами (должностными обязанностями).

В приказе (распоряжении, указании) о работе гражданина на постоянной основе со сведениями, составляющими государственную тайну, указываются должность (звание) гражданина, его фамилия, имя, отчество, дата оформления и номер допуска к сведениям, составляющим государственную тайну, размер устанавливаемой процентной надбавки. Приказ (распоряжение, указание) издается не реже одного раза в год. Приказ (распоряжение, указание) издается также при внесении изменений в штатное расписание (штат), номенклатуру должностей работников, подлежащих оформлению на допуск к государственной тайне, в случае изменения формы допуска граждан к государственной тайне, при приеме граждан на работу (службу) и их увольнении.

Руководителям федеральных государственных органов и их заместителям, руководителям территориальных органов федеральных государственных органов и их заместителям, а также

руководителям организаций размеры процентной надбавки за работу со сведениями, составляющими государственную тайну, устанавливаются представителем нанимателя или лицами, на которых возложены полномочия представителя нанимателя по заключению служебных контрактов о прохождении федеральной государственной гражданской службы, в соответствии с их полномочиями.

Руководителям организаций, подведомственных государственным органам и органам местного самоуправления, не являющимся государственными служащими или муниципальными служащими, а также руководителям организаций, для которых ведомственная подчиненность не определена, размер процентной надбавки за работу со сведениями, составляющими государственную тайну, устанавливается трудовым договором исходя из высшей степени секретности работ, проводимых данной организацией.

За время нахождения в оплачиваемом отпуске, служебной командировке, на излечении амбулаторно и в лечебном учреждении и в других случаях, когда в соответствии с законодательством Российской Федерации гражданину сохраняется (выплачивается) средняя заработная плата (денежное содержание, денежное довольствие), процентная надбавка за работу со сведениями, составляющими государственную тайну, учитывается в составе среднего заработка (денежного содержания, денежного довольствия), сохраняемого (выплачиваемого) за эти периоды.

Доплаты, надбавки, повышения (увеличения) должностных окладов (тарифных ставок) гражданам, допущенным к государственной тайне на постоянной основе, и коэффициенты, носящие компенсационный характер (за работу на специальных или режимных объектах, за участие в выполнении работ по специальным программам, работникам, занятым на шифровальной и дешифровальной работах, и другие аналогичные работы), применяются в ранее установленных нормативными правовыми актами порядке и размерах.

Процентная надбавка за работу со сведениями, составляющими государственную тайну, не выплачивается:

– гражданам, освобожденным от занимаемых должностей;

– гражданам, в отношении которых допуск к государственной тайне на постоянной основе прекращен;

– гражданам, освобожденным от работы на постоянной основе со сведениями, составляющими государственную тайну, приказом (распоряжением, указанием);

– гражданам, находящимся в отпуске по уходу за ребенком до достижения им установленного возраста;

– военнослужащим и лицам рядового и начальствующего состава, находящимся в распоряжении соответствующих командиров (начальников);

– гражданам, находящимся в отпуске без сохранения заработной платы (денежного содержания, денежного довольствия).

Выплата процентной надбавки за работу со сведениями, составляющими государственную тайну, прекращается со дня, следующего за днем освобождения от должности, прекращения допуска к государственной тайне на постоянной основе, освобождения от работы на постоянной основе со сведениями, составляющими государственную тайну.

Сотрудникам структурных подразделений по защите государственной тайны государственных органов, органов местного самоуправления, организаций, воинских частей (далее – структурные подразделения по защите государственной тайны) дополнительно к процентной надбавке, предусмотренной п. 1 правил, устанавливается ежемесячная процентная надбавка к должностному окладу (тарифной ставке) за стаж работы в соответствии с п. 3 правил.

Структурными подразделениями по защите государственной тайны считаются созданные в соответствии с законодательством Российской Федерации специальные подразделения, а также отдельные должности, замещаемые специалистами, основной функцией которых является обеспечение защиты государственной тайны.

Перечень структурных подразделений и отдельных должностей по защите государственной тайны утверждается приказами

(распоряжениями, указаниями). В перечень включаются только те структурные подразделения и отдельные должности, на которые согласно утвержденным в установленном порядке положениям (должностным регламентам, должностным обязанностям) возложено выполнение конкретных задач (функций) с учетом специфики проводимых работ по защите государственной тайны, предусмотренных нормативными правовыми актами Российской Федерации, в качестве их основных функций.

При определении стажа работы (службы) в структурных подразделениях по защите государственной тайны учитывается только подтвержденный документально стаж работы (службы) в указанных подразделениях независимо от того, в каком государственном органе, органе местного самоуправления, организации, воинской части работал (служил) сотрудник. При этом перерывы в работе (службе) в структурных подразделениях по защите государственной тайны в стаж работы (службы) для получения процентной надбавки за стаж работы (службы) в структурных подразделениях по защите государственной тайны не засчитываются.

Выплата процентной надбавки за стаж работы (службы) производится на основании приказа (распоряжения, указания) в соответствии с полномочиями.

Процентные надбавки за работу со сведениями, составляющими государственную тайну, и за стаж работы в структурных подразделениях по защите государственной тайны включаются в состав заработной платы, на которую начисляются районные коэффициенты, коэффициенты за работу в высокогорных районах, пустынных и безводных местностях и процентная надбавка к заработной плате лицам, работающим в районах Крайнего Севера, приравненных к ним местностях, в южных районах Дальнего Востока, Красноярского края, Иркутской и Читинской областей, Республики Бурятия, в Республике Хакасия.

В случае, если размер ежемесячной процентной надбавки за работу со сведениями, составляющими государственную тайну, к должностному окладу (тарифной ставке) оказывается ниже размера ранее установленной надбавки, получаемой гражданами,

допущенными к государственной тайне на постоянной основе, за работу со сведениями, составляющими государственную тайну, им сохраняется ранее установленная надбавка до истечения срока договора (контракта), которым она предусмотрена.

В соответствии с Постановлением Совета Народных Комиссаров Союза ССР от 17.04.1939 № 22 работникам структурных подразделений по защите государственной тайны установлен ежегодно месячный отпуск.

2.6. Ответственность за нарушение законодательства Российской Федерации о государственной тайне

Общая тайна, которой ни с кем другим нельзя поделиться,
связывает прочнее общего дела или общего интереса.

Левиафиан (Акунин)

Тайна имеет свойство молодого вина,
которое постоянно грозит взорвать бутылку.

Моисей Сафир

В соответствии со ст. 26. Закона РФ от 21.07.1993 № 5485-1 (ред. от 29.07.2018) «О государственной тайне» должностные лица и граждане, виновные в нарушении законодательства Российской Федерации о государственной тайне, несут уголовную, административную, гражданско-правовую или дисциплинарную ответственность в соответствии с действующим законодательством.

Соответствующие органы государственной власти и их должностные лица основываются на подготовленных в установленном порядке экспертных заключениях об отнесении незаконно распространенных сведений к сведениям, составляющим государственную тайну.

Рис. 2.12. Виды ответственности за нарушение законодательства о государственной тайне

Защита прав и законных интересов граждан, органов государственной власти, предприятий, учреждений и организаций в сфере действия настоящего Закона осуществляется в судебном или ином порядке, предусмотренном настоящим Законом.

Нарушение законодательства о государственной тайне может совершаться как умышленно, так и неосторожно. За нарушение законодательства о государственной тайне предусмотрены виды ответственности (рис. 2.12).

За умышленное нарушение законодательства о государственной тайне в виде государственной измены, шпионажа, разглашения государственной тайны предусмотрена *уголовная ответственность* ст. 275, 276, 283 УК РФ соответственно. Также уголовная ответственность предусмотрена и за такое деяние, как утрата документов, содержащих государственную тайну, ст. 284 УК РФ. Однако это преступление совершается с неосторожной формой вины.

Нарушение правил защиты информации и незаконная деятельность в области защиты информации могут совершаться как умышленно, так и неосторожно и влекут административную ответственность, предусмотренную ст. 13.12, 13.13 КоАП РФ.

При совершении должностным лицом указанных уголовно или административно наказуемых деяний для него также наступает дисциплинарная ответственность, которая заключается, как правило, в увольнении виновного лица по соответствующему основанию, предусмотренному ст. 81 ТК РФ:

– либо по пп. «в» п. 6 – в связи с однократным грубым нарушением работником трудовых обязанностей, выразившемся

в разглашении охраняемой законом государственной тайны, ставшей известной работнику в связи с исполнением им трудовых обязанностей;

– либо по п. 10 – в связи с однократным грубым нарушением руководителем организации (филиала, представительства), его заместителями своих трудовых обязанностей;

– либо по п. 12 – в связи с прекращением допуска к государственной тайне, если выполняемая работа требует допуска к государственной тайне.

Увольнение по соответствующему пункту производится в зависимости от конкретных обстоятельств дела.

При решении вопросов о привлечении должностных лиц и граждан к какой-либо ответственности органы государственной власти и их должностные лица должны назначить экспертизу, на разрешение которой поставить вопрос о том, относятся ли сведения, порядок работы с которыми был нарушен, к сведениям, составляющим государственную тайну. Экспертиза проводится должностными лицами того ведомства (или тех ведомств), к ведению которых могут быть отнесены исследуемые сведения по их содержанию либо по ведомственной принадлежности предприятия, учреждения, организации, где они были получены или разработаны.

Возбуждение административных дел и производство по ним осуществляется:

1. Директором ФСБ, его заместителями, руководителями территориальных органов ФСБ, их заместителями.

2. Министром обороны, его заместителями.

3. Директором СВР, его заместителями.

4. Председателем Федеральной службы по техническому и экспортному контролю России, его заместителями, руководителями региональных центров, их заместителями.

5. Руководителями структурных подразделений ФСБ, Минобороны, СВР и Федеральной службы по техническому и экспортному контролю России, к ведению которых отнесено лицензирование видов деятельности, связанных с использованием и защитой сведений, составляющих государственную тайну.

В соответствии с ч. 2 ст. 23.1 КоАП указанные должностные лица вправе передавать дела об административных правонарушениях, предусмотренных ч. 4 ст. 13.12 КоАП РФ, и ч. 2 ст. 13.13 КоАП РФ на рассмотрение судьям. Последнее право реализуется должностными лицами при наличии по обстоятельствам дела необходимости применить к лицу, обвиняемому в совершении административного правонарушения, вида наказания, который может назначать только суд, например конфискация имущества.

Часть 3 ст. 13.12 КоАП РФ предусматривает ответственность за 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, что 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.

Часть 4 этой же статьи предусматривает ответственность за использование несертифицированных средств, предназначенных для защиты информации, составляющей государственную тайну, что влечет наложение административного штрафа:

– на должностных лиц – в размере от тридцати до сорока минимальных размеров оплаты труда;

– на юридических лиц – от двухсот до трехсот минимальных размеров оплаты труда с конфискацией несертифицированных средств, предназначенных для защиты информации, составляющей государственную тайну, или без таковой.

Субъектами указанных административных правонарушений могут быть должностные лица и юридические лица.

Часть 2 ст. 13.13 КоАП РФ предусматривает ответственность за занятие видами деятельности, связанной 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, без лицензии, что влечет наложение административного штрафа:

– на должностных лиц – в размере от сорока до пятидесяти минимальных размеров оплаты труда;

– на юридических лиц – от трехсот до четырехсот минимальных размеров оплаты труда с конфискацией созданных без лицензии средств защиты информации, составляющей государственную тайну, или без таковой.

Общий порядок наложения *дисциплинарных взысканий* регулируется ст. 193 ТК РФ. В соответствии с указанной статьей Закона до применения дисциплинарного взыскания работодатель должен затребовать от работника объяснение в письменной форме. В случае отказа работника дать указанное объяснение составляется соответствующий акт.

Дисциплинарное производство в отношении работника, нарушившего законодательство о государственной тайне, может проводить как непосредственно сам работодатель, так и специально уполномоченное им для этого лицо, которое по результатам проверки собранные материалы вместе со своим заключением передает работодателю.

Отказ работника дать объяснение не является препятствием для применения дисциплинарного взыскания.

Дисциплинарное взыскание применяется не позднее одного месяца со дня обнаружения проступка, не считая времени болезни работника, пребывания его в отпуске, а также времени, необходимого на учет мнения представительного органа работников.

Дисциплинарное взыскание не может быть применено позднее шести месяцев со дня совершения проступка. В указанный срок не включается время производства по уголовному делу.

За каждый дисциплинарный проступок может быть применено только одно дисциплинарное взыскание.

Приказ (распоряжение) работодателя о применении дисциплинарного взыскания объявляется работнику под расписку

в течение трех рабочих дней со дня его издания. В случае отказа работника подписать указанный приказ (распоряжение) составляется соответствующий акт.

Дисциплинарное взыскание может быть обжаловано работником в государственных инспекциях труда или органах по рассмотрению индивидуальных трудовых споров.

С учетом серьезности возможных последствий нарушения законодательства о государственной тайне к работникам, допустившим такое нарушение, применяется, как правило, дисциплинарное наказание в виде увольнения по соответствующему основанию.

Уголовный кодекс РФ устанавливает уголовную ответственность за восемь видов посягательств на государственную тайну:

– шпионаж (ст. 275 и 276 УК РФ);

– выдача государственной тайны иностранному государству, иностранной организации или их представителям (ст. 275 УК РФ);

– иное оказание помощи иностранному государству, организации или их представителям (ст. 275 УК РФ);

– разглашение государственной тайны (ст. 283 УК РФ);

– утрата документов, содержащих государственную тайну, предметов, сведения о которых составляют государственную (ст. 284 УК РФ);

– уничтожение, блокирование, модификация или копирование охраняемой законом компьютерной информации (в том числе содержащей государственную тайну) в результате неправомерного доступа к ней (ст. 272 УК РФ) или нарушения правил эксплуатации ЭВМ, системы ЭВМ или их сети (ст. 274 УК РФ);

– постановление охраняемой законом компьютерной информации (в том числе содержащей государственную тайну) в заведомую опасность несанкционированного уничтожения, блокирования или копирования в результате создания или распространения вредоносных программ для ЭВМ (ст. 273 УК РФ);

– похищение, уничтожение, повреждение или сокрытие официальных документов (в том числе содержащих государственную тайну) (ч. 1 ст. 325 УК РФ).

Статья 13.14. Разглашение информации с ограниченным доступом

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.

Защита государственной тайны является важной составной частью обеспечения безопасности личности, общества и государства, причем речь идет фактически об охране всех сфер безопасности, включая, в частности, политическую, военную, экономическую и информационную. В связи с этим защита государственной тайны требует использования широкого спектра государственных мер, включая меры уголовно-правового характера.

Уголовно-правовая защита информации, составляющей государственную тайну, согласно нормам действующего УК РФ, осуществляется с помощью введения уголовно-правового запрета на совершение ряда деяний (действий или бездействия), предметом посягательства которых выступает государственная тайна, т. е. объявление таких деяний преступными, уголовно наказуемыми, и установления за них различных мер наказания, а также с помощью некоторых поощрительных норм, направленных на минимизацию последствий такого рода посягательств.

Непосредственно защите государственной тайны посвящены: ст. 275 («Государственная измена»), ст. 276 («Шпионаж»), ст. 283 («Разглашение государственной тайны») и ст. 284 УК РФ («Утрата документов, содержащих государственную тайну»).

Статья 275. Государственная измена

Государственная измена, т. е. шпионаж, выдача государственной тайны либо иное оказание помощи иностранному государству, иностранной организации или их представителям в проведении враждебной деятельности в ущерб внешней безопасности Российской Федерации, совершенная гражданином

Российской Федерации, – наказывается лишением свободы на срок от двенадцати до двадцати лет со штрафом в размере до пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до трех лет или без такового.

Лицо, совершившее преступления, предусмотренные настоящей статьей, а также ст. 276 и 278 нестоящего Кодекса, освобождается от уголовной ответственности, если оно добровольным и своевременным сообщением органам власти или иным образом способствовало предотвращению дальнейшего ущерба интересам Российской Федерации и если в его действиях не содержится иного состава преступления.

Статья 276. Шпионаж

Передача, а равно собирание, похищение или хранение в целях передачи иностранному государству, иностранной организации или их представителям сведений, составляющих государственную тайну, а также передача или собирание по заданию иностранной разведки иных сведений для использования их в ущерб внешней безопасности Российской Федерации, если эти деяния совершены иностранным гражданином или лицом без гражданства, наказывается лишением свободы на срок от десяти до двадцати лет.

Статья 283. Разглашение государственной тайны

1. Разглашение сведений, составляющих государственную тайну, лицом, которому она была доверена или стала известна по службе или работе, если эти сведения стали достоянием других лиц, при отсутствии признаков государственной измены – наказывается арестом на срок от четырех до шести месяцев либо лишением свободы на срок до четырех лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового.

2. То же деяние, повлекшее по неосторожности тяжкие последствия, — наказывается лишением свободы на срок от трех до семи лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет.

Следует иметь в виду, что Федеральным законом от 27.07.2006 № 153-ФЗ Уголовный кодекс Российской Федерации дополнен

гл. 15.1 «Конфискация имущества», которая включает ст. 104.1, 104.2 и 104.3. Как видно из текста этой главы, конфискация имущества не является мерой наказания, а относится к иным мерам уголовно-правового характера.

Статья 284. Утрата документов, содержащих государственную тайну

Нарушение лицом, имеющим допуск к государственной тайне, установленных правил обращения с содержащими государственную тайну документами, а равно с предметами, сведения о которых составляют государственную тайну, если это повлекло по неосторожности их утрату и наступление тяжких последствий, — наказывается ограничением свободы на срок до трех лет либо арестом на срок от четырех до шести месяцев, либо лишением свободы на срок до трех лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового.

Кроме вышеприведенных статей в УК РФ включен еще ряд норм, направленных на защиту охраняемой законом информации. При этом под охраняемой законом информацией понимаются различные не подлежащие несанкционированному распространению сведения, в число которых наряду с другими данными (например, содержащими личную, семейную, коммерческую, банковскую, налоговую, служебную, профессиональную и другую тайну) входит и информация, составляющая тайну государственную. Эти нормы предусматривают уголовную ответственность за неправомерный доступ к компьютерной информации (ст. 272), создание, использование и распространение вредоносных программ для ЭВМ (ст. 273), нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети (ст. 274) и за похищение или повреждение документов, штампов, печатей (ч. 1 ст. 325 УК РФ).

Статья 272. Неправомерный доступ к компьютерной информации

1. 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 двухсот тысяч рублей 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.

2. 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 до трехсот тысяч рублей 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.

Статья 273. Создание, использование и распространение вредоносных программ для ЭВМ

1. 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 – наказывается лишением свободы на срок от двух до трех лет со штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев.

2. Те же деяния, повлекшие по неосторожности тяжкие последствия, — наказываются лишением свободы на срок от трех до семи лет.

Статья 274. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети

1. 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 ста восьмидесяти до двухсот сорока часов, либо ограничением свободы на срок до двух лет.

2. То же деяние, повлекшее по неосторожности тяжкие последствия, — наказывается лишением свободы на срок до четырех лет.

Статья 325. Похищение или повреждение документов, штампов, печатей

Похищение, уничтожение, повреждение или сокрытие официальных документов, штампов или печатей, совершенные из корыстной или иной личной заинтересованности, – наказывается штрафом в размере до двухсот тысяч рублей или в размере заработной платы, или иного дохода, осужденного за период до восемнадцати месяцев, либо исправительными работами на срок до двух лет, либо арестом на срок до четырех месяцев, либо лишением свободы на срок до одного года.

Уголовная ответственность предусмотрена за посягательство на государственную тайну, независимо от того, к какой области (военной, экономической, научно-технической, внешнеполитической, внешнеэкономической, разведывательной, контрразведывательной или оперативно-разыскной деятельности) и к какой степени секретности (особой важности, совершенно секретным или секретным) относятся сведения, составляющие государственную тайну. Область государственной деятельности и степень секретности учитываются при назначении наказания за соответствующее посягательство. При назначении наказания учитываются также и последствия, к которым привело конкретное посягательство на государственную тайну.

Шпионаж

Как следует из текста ст. 275 и 276 УК РФ, на государственную тайну посягает **шпионаж первого вида**, *который заключается в передаче, а равно в собирании, похищении или хранении в целях передачи иностранному государству, иностранной организации или их представителям такого рода секретной информации*.

В отличие от шпионажа первого вида, **шпионаж второго вида** *состоит в передаче или собирании по заданию иностранной разведки иных сведений, т. е. не составляющих государственной тайны, для использования в ущерб внешней безопасности Российской Федерации*. Таким образом, шпионаж второго вида не является посягательством на государственную тайну: он посягает на другую информацию.

Вместе с тем следует иметь в виду, что иные сведения, хотя и не составляют сами по себе государственной тайны, зачастую используются иностранными разведками для обобщения, анализа, сопоставления с уже имеющейся информацией, что позволяет спецслужбам получить новые данные, которые в совокупности образуют государственную тайну. Кроме того, полученные от изменника или шпиона-иностранца иные сведения могут служить зарубежной разведке для уточнения, проверки, пополнения уже имеющейся в ее распоряжении информации, относящейся к государственной тайне. Так, в судебно-следственной практике неоднократно отмечались факты, когда зарубежные разведки давали своим агентам задания добывать в определенных регионах нашей страны образцы почвы, воды, флоры и фауны, чтобы в дальнейшем путем исследования этих фрагментов получить информацию о местонахождении в данной местности интересующих спецслужбу объектов и характере их деятельности.

Предметом посягательства при совершении шпионажа первого вида являются сведения, составляющие государственную тайну, т. е. информация, под которой, согласно п. 1 ст. 2 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», понимаются сведения (сообщения, данные) независимо от формы их представления. Информация в таком понимании является предметом шпионажа первого вида при передаче и собирании сведений, составляющих государственную тайну.

При похищении сведений предметом посягательства выступает документированная информация, которая, как разъясняется в п. 11 той же ст. 2 Федерального закона от 27.07.2006

№ 149-ФЗ, представляет собой информацию, зафиксированную на материальном носителе путем документирования с реквизитами, позволяющими определить такую информацию, или сам материальный носитель подобной информации. Согласно ст. 2 Закона РФ «О государственной тайне», такими носителями являются материальные объекты, в том числе физические поля, в которых сведения, составляющие государственную тайну, находят свое отображение в виде символов, образов, сигналов, технических решений и процессов. При хранении сведений субъект посягает на информацию, которая содержится на материальном носителе, причем эта информация может быть снабжена реквизитами, т. е. относиться к документированной, а может также и не иметь этих отличительных признаков.

При этом информация, зафиксированная на материальном носителе (как документированная, так и не снабженная реквизитами), может быть предметом посягательства не только при похищении и хранении, но и при передаче или собирании сведений, составляющих государственную тайну.

Представители иностранных государств или зарубежных организаций могут открыто представлять их либо действовать конспиративно, на конфиденциальной основе. Представители иностранного государства или зарубежной организации могут являться гражданами данного государства либо какой-то третьей страны, лицами без гражданства, а иногда и гражданами Российской Федерации.

Выдача государственной тайны

Выдача государственной тайны является одной из форм государственной измены (ст. 275 УК РФ). Ответственность за его совершение несут только граждане Российской Федерации. Наказание за выдачу государственной тайны установлено такое же, как и за шпионаж, совершенный российским гражданином. Установление особой ответственности за это деяние для граждан Российской Федерации является несправедливым и противоречит положениям ст. 19 (ч. 1) Конституции Российской Федерации.

*Предмет **посягательства** и «адресаты» у данного преступления — такие же, как у шпионажа первого вида, однако в объективную сторону*

состава этого деяния не включаются собирание, похищение или хранение сведений, составляющих государственную тайну, в целях передачи иностранному государству, иностранной организации или их представителям. Объективная сторона преступления сводится только к одному элементу – выдаче государственной тайны иностранному государству, иностранной организации или их представителям. Выдача государственной тайны может осуществляться теми же способами, как и передача таких же сведений при совершении шпионажа первого вида. Составляющие государственную тайну сведения при этом могут выступать как в виде документированной, так и недокументированной информации.

Иное оказание помощи иностранному государству, иностранной организации или их представителям в проведении враждебной деятельности в ущерб внешней безопасности Российской Федерации представляет собой ***третью форму государственной измены*** (ст. 275 УК РФ). За совершение данного преступления несут ответственность только российские граждане, что, как и в отношении первых двух форм государственной измены, представляется анахронизмом, противоречащим мировому опыту и положениям ст. 19 (ч. 1) Конституции Российской Федерации.

Иное оказание помощи означает такое содействие иностранному государству, иностранной организации или их представителям в проведении враждебной деятельности в ущерб внешней безопасности Российской Федерации, которое не охватывается двумя остальными формами государственной измены, т. е. шпионажем (обоих видов) и выдачей государственной тайны.

Другими словами, к иному оказанию помощи относятся все деяния, совершенные виновным в сговоре с иностранным государством, иностранной организацией или их представителем, которые, с одной стороны, направлены в ущерб внешней безопасности России, а с другой, – выходят за рамки передачи и выдачи «адресатам» сведений, составляющих государственную тайну, собирания, похищения или хранения тех же сведений в целях их передачи тем же «адресатам» либо передачи или собирания по заданию иностранной разведки иных сведений для их использования в ущерб внешней безопасности РФ.

Поскольку шпионаж (обоих видов) и выдача государственной тайны перечисленным в законе «адресатам» представляют собой всего лишь разновидности оказания тем же «адресатам» помощи в проведении враждебной деятельности в ущерб внешней безопасности России, то третью из числа указанных в ст. 275 УК РФ форм государственной измены, т. е. оказание помощи, следует рассматривать как основную форму названного преступления, ответственность за совершение которой наступает в том случае, если отсутствуют обязательные признаки двух других разновидностей государственной измены.

Разглашение государственной тайны

Ответственность за разглашение государственной тайны предусмотрена ст. 283 УК РФ, которая состоит из двух частей.

Согласно ч. 1 ст. 283 УК РФ наказывается «разглашение сведений, составляющих государственную тайну, лицом, которому она была доверена или стала известна по службе или работе, если эти сведения стали достоянием других лиц, при отсутствии признаков государственной измены».

Предметом посягательства при разглашении государственной тайны выступает как документированная, так и недокументированная информация, составляющая такую тайну.

Разглашение сведений, составляющих государственную тайну, состоит в несанкционированном распространении указанных сведений, доведении их содержания до лиц, которые не имеют права на законном основании знакомиться с ними. Разглашение может быть осуществлено устно, письменно, путем предоставления для ознакомления документов, других материальных носителей информации, чертежей, моделей, приборов, устройств, изделий, материалов и т. д., путем опубликования сведений в средствах массовой информации, передачи по радио, телефону, телеграфу, телевидению, факсу, компьютерной сети и т. п.

Утрата документов, содержащих государственную тайну, или предметов, сведения о которых составляют государственную тайну

Ответственность за это преступление предусмотрена ст. 284 УК РФ.

Предметом посягательства при совершении этого преступления выступают содержащие государственную тайну документы, а также предметы, сведения о которых составляют государственную тайну, т. е. исключительно документированная информация. Таким образом, предмет посягательства должен иметь следующие признаки:

– признак материальности, т. е. являться материальным носителем информации. По материальному признаку документами являются текстовые и графические материалы, выполненные любым способом, магнитные ленты, перфорированные ленты и карты, кино-, фотонегативы, компьютерные дискеты и другие объекты. К предметам относятся изделия, их части (блоки, агрегаты, приборы) и вещества;

– признак информативности, согласно которому предметом посягательства при совершении данного преступления являются лишь документы, содержащие государственную тайну, или предметы, сведения о которых составляют государственную тайну.

Наличие государственной тайны в сведениях, содержащихся в документе или предмете, определяется путем сопоставления фактической информации со специально установленными перечнями. Оценка степени секретности этих сведений должна соответствовать их фактическому содержанию. Ее расхождение с содержанием недопустимо.

Отсутствие в сведениях государственной тайны свидетельствует о том, что нет и предмета посягательства применительно к ст. 284 УК РФ. На практике такие несоответствия возникают неоднократно, что объясняется рядом объективных и субъективных причин. К числу объективных факторов, влияющих на снижение степени секретности сведений, относятся появление новых достижений науки и техники, снятие изделия с вооружения, издание нового документа и т. п. К субъективным факторам следует отнести, например, ошибки лиц, определяющих степень секретности информации. В связи с этим для получения достоверной оценки степени секретности утраченного документа (предмета) мало одного грифа секретности, необходимо:

– заключение компетентных специалистов (экспертов);

– удостоверительный признак, который является свидетельством включения конкретного документа или предмета в систему отношений по защите как содержащейся в них государственной тайны, так и их самих.

Уничтожение, блокирование, модификация или копирование охраняемой законом компьютерной информации (в том числе содержащей государственную тайну)

Уголовная ответственность за такого рода посягательства на государственную тайну, которая в этих случаях выступает в качестве одной из разновидностей охраняемой законом компьютерной информации, предусмотрена ст. 272 и 274 УК РФ.

Предметом посягательства при совершении названных деяний является охраняемая законом компьютерная информация.

Компьютерная информация, в соответствии с ч. 1 ст. 272 УК РФ, – это информация на машинном носителе, в электронно-вычислительной машине (ЭВМ, компьютере), системе ЭВМ или их сети. Таким образом, компьютерная информация представляет собой разновидность документированной информации, зафиксированной на специальном машинном носителе или в ЭВМ (системе ЭВМ, их сети). Вместе с тем следует помнить, что предметом посягательства при совершении рассматриваемых преступлений выступает не любая компьютерная информация, а лишь охраняемая законом.

Согласно ст. 5 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», информация в зависимости от порядка ее предоставления или распространения подразделяется на:

– информацию, свободно распространяемую;

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

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

– информацию, распространение которой в Российской Федерации ограничивается или запрещается.

В соответствии со ст. 9 названного Федерального закона ограничение доступа к информации устанавливается федеральными законами в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны и безопасности государства. В ст. 9 перечисляются виды информации, подлежащие защите. Это сведения, составляющие государственную, коммерческую, служебную, профессиональную тайну, а также личную и семейную тайну.

Сведения, составляющие государственную тайну, являются лишь частью охраняемой законом информации, посягательства на которую предусмотрены в ст. 272-274 УК РФ. В связи с этим необходимо помнить, что когда деяния, о которых говорится в названных статьях, имеют признаки государственной измены, шпионажа или разглашения государственной тайны, ответственность должна наступать по принципу совокупности преступлений, т. е. не только за посягательство на охраняемую законом компьютерную информацию, но и за соответствующее посягательство на государственную тайну по ст. 275, 276 или 283 УК РФ.

Статья 272 УК РФ «Неправомерный доступ к компьютерной информации» состоит из двух частей. Согласно ч. 1 ст. 272 УК РФ установлено наказание за неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети.

Объективная сторона деяния сконструирована применительно к преступлениям с так называемым материальным составом и включает в себя:

– неправомерный доступ к охраняемой законом компьютерной информации, под которым понимается незаконное получение возможности сбора, накопления, поиска и распространения информации, на которую у виновного нет права;

– наступление вредных последствий в виде уничтожения, блокирования, модификации либо копирования информации, нарушения работы ЭВМ, системы ЭВМ или их сети;

– причинную связь между неправомерным доступом к компьютерной информации и наступившими вредными последствиями.

Под уничтожением компьютерной информации понимается приведение ее в состояние, когда она не может быть восстановлена и использована по назначению.

Блокирование компьютерной информации состоит в создании невозможности ее получения или использования по назначению при полной сохранности самой информации.

Модификацией компьютерной информации называются любые ее изменения, не направленные на обеспечение интересов собственника или иного владельца информации.

Копирование компьютерной информации означает ее воспроизводство в любой материальной форме, за исключением получения ее из изображения на дисплее компьютера.

Нарушение работы ЭВМ, системы ЭВМ или их сети заключается в создании помех нормальному функционированию компьютера, системы ЭВМ или их сети, перерыве их работы или полном ее прекращении.

Преступление характеризуется умышленной виной, причем умысел может быть прямым и косвенным.

В ч. 2 ст. 272 УК РФ предусматривается ответственность за то же деяние, но совершенное при отягчающих обстоятельствах. Отягчающими обстоятельствами считаются совершение преступления:

– группой лиц по предварительному сговору, т. е. если в нем участвовали лица, заранее договорившиеся о совместном совершении преступления (ч. 2 ст. 35 УК РФ);

– организованной группой лиц, т. е. если оно совершено устойчивой группой лиц, заранее объединившихся для совершения одного или нескольких преступлений (ч. 3 ст. 35 УК РФ);

– лицом с использованием своего служебного положения, а равно имеющим доступ к ЭВМ, системе ЭВМ или их сети. Использование служебного положения при совершении этого деяния состоит в том, сто виновный получает доступ к компьютерной информации, незаконно используя права, предоставленные

ему исключительно в силу выполняемой им служебной деятельности.

Доступ к ЭВМ, системе ЭВМ или их сети, как правило, имеет лицо в силу выполняемой им работы, ввязанной с эксплуатацией или обслуживанием компьютера, компьютерной системы или их сети (далеко не всякое лицо, имеющее право доступа к компьютерной информации, имеет непосредственный доступ к ЭВМ, компьютерной системе или их сети, точно так же, как не всякий, кто имеет доступ к ЭВМ, системе ЭВМ или их сети, имеет право пользоваться заключенной в них информацией).

В ст. 274 УК РФ, которая также состоит из двух частей, рассматриваются примерно такие же посягательства на охраняемую законом компьютерную информацию, что и в ст. 272 УК РФ, за исключением копирования информации и нарушения работы ЭВМ, системы ЭВМ или их сети, однако предусматриваются иные способы осуществления таких посягательств, чем в ст. 272 УК РФ.

Объективная сторона деяния, о котором говорится в ч. 1 ст. 274 УК РФ, характеризует его как преступление с материальным составом. Его объективная сторона включает в себя совокупность следующих элементов:

– нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети, под которым понимается нарушение установленных правил, касающихся эксплуатации аппаратного обеспечения ЭВМ, системы ЭВМ или их сети либо программного обеспечения, предназначенного для функционирования тех же компьютерных устройств;

– наступление вредных последствий в виде уничтожения, блокирования или модификации охраняемой законом компьютерной информации;

– причинение в результате этих негативных последствий существенного вреда интересам собственника, владельца или пользователя компьютерной информации, причем решение о том, является ли причиненный вред существенным, принимается судом с учетом всех обстоятельств дела;

– причинная связь между нарушением правил эксплуатации, наступившими последствиями (уничтожением, блокированием

или модификацией информации) и существенным вредом, который повлекли указанные последствия.

Преступление считается оконченным с момента наступления перечисленных последствий и причинения существенного вреда.

Субъект данного преступления специальный – лицо, имеющее доступ к ЭВМ, системе ЭВМ или их сети по работе, связанной с их эксплуатацией или обслуживанием. Нарушение правил эксплуатации является умышленным преступлением: виновный осознает, что нарушает правила эксплуатации, предвидит неизбежность или возможность уничтожения, блокирования или модификации компьютерной информации и причинения в результате этого существенного вреда и либо сознательно допускает такие последствия, либо относится к ним безразлично.

По ч. 2 ст. 274 УК РФ наказывается то же деяние, повлекшее по неосторожности тяжкие последствия.

Вопрос о том, являются ли наступившие последствия тяжкими, решается судом. Как тяжкие могут быть оценены такие последствия, как крупный материальный вред, остановка того или иного предприятия, учреждения, перерыв в их работе и т. п.

В случае наступления тяжких последствий действия виновного квалифицируются по ч. 2 ст. 274 УК РФ в том случае, если он относился к ним неосторожно, т. е. легкомысленно или небрежно. Когда же субъект умышленно причиняет вред, оцениваемый как тяжкий, он должен нести ответственность по ч. 1 ст. 274 УК РФ и (по совокупности) по той статье УК, которая предусматривает умышленное причинение того преступного результата, который имел место в данном конкретном случае.

Поставление охраняемой компьютерной информации (в том числе составляющей государственную тайну) в заведомую опасность несанкционированного уничтожения, блокирования, модификации либо копирования

Данное преступление предусмотрено ст. 273 УК РФ, состоящей из двух частей. Согласно ч. 1 ст. 273 УК РФ установлена уголовная ответственность за 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 за использование либо распространение таких программ или машинных носителей с такими программами.

Объективную сторону преступления образует совершение любого из следующих шести деяний:

– создание программ для ЭВМ (компьютерных программ), т. е. проведение деятельности, в результате которой осуществляется предоставление в объективной форме совокупности данных и команд, предназначенных для функционирования ЭВМ и других электронных устройств;

– внесение в существующие компьютерные программы изменений, т. е. модификация (переработка) программ для ЭВМ и других электронных устройств;

– использование компьютерных программ, т. е. выпуск их в свет, воспроизведение, распространение и иные действия по их введению в хозяйственный оборот;

– распространение компьютерных программ, т. е. предоставление доступа к воспроизведенной в любой форме программе для ЭВМ, в том числе сетевым и иными способами, а также путем продажи, проката, сдачи внаем, предоставления взаймы, включая импорт для любой из этих целей;

– использование машинных носителей с компьютерными программами;

– распространение машинных носителей с компьютерными программами.

При этом использование и распространение машинных носителей с компьютерными программами осуществляется теми же способами, что и использование или распространение самих программ. Обязательным элементом объективной стороны рассматриваемого преступления является специфический предмет – программа-вирус, т. е. такая программа, которая «заражает» ЭВМ, системы ЭВМ или их сеть, в результате чего на компьютере выполняются различные нежелательные действия либо создаются

помехи для ожидаемых действий. Ответственность по ст. 273 УК РФ наступает только при создании вредоносных программ, внесении в существующие программы такого рода изменений, а также при иных манипуляциях с подобными программами, ставящими компьютерную информацию или компьютерные устройства в опасность нежелательного функционирования.

В ч. 1 ст. 273 УК РФ конкретно указываются эти нежелательные несанкционированные действия и помехи:

– уничтожение компьютерной информации;

– блокирование компьютерной информации;

– модификация компьютерной информации;

– копирование компьютерной информации;

– нарушение работы ЭВМ, системы ЭВМ или их сети.

Похищение, уничтожение, повреждение или сокрытие официальных документов, в том числе содержащих государственную тайну

Как и в ст. 272-274 УК РФ, уголовно-правовой запрет, установленный в ч. 1 ст. 325 УК РФ, направлен на защиту не только государственной тайны, но и любой информации, содержащейся в официальных документах, т. е. документированной информации, а также и самих официальных документов.

Предметом посягательства в данном случае являются официальные документы:

– выданные государственным органом, адресованные ему;

– выданные негосударственной организацией в пределах ее компетенции;

– документы частного характера (доверенности, расписки, договоры), если они засвидетельствованы в нотариальном или ином установленном законом официальном порядке.

Кроме того, предметом посягательства по ч. 1 ст. 325 УК РФ признаются штампы и печати.

Объективная сторона разбираемого преступления включает в себя следующие посягательства на упомянутый предмет:

– похищение, т. е. любое ненасильственное незаконное завладение документом способом, характерным для хищения (тайно, открыто, путем обмана и т. п.). В случае применения

насилия при завладении официальными документами содеянное квалифицируется не только по ч. 1 ст. 325 УК РФ, но также (в зависимости от характера примененного насилия) и по соответствующим статьям, предусматривающим преступления против жизни и здоровья (гл. 16 УК РФ), или по ст. 318 УК РФ (применение насилия в отношении представителя власти);

– уничтожение документов – любые действия, в результате которых документы были полностью истреблены;

– повреждение документов — причинение им вреда, в результате которого они не могут быть использованы по назначению. Умышленное повреждение документа, изменяющее его содержание (например, отрывание части документа с текстом, заливание части текста чернилами, вытравливание фрагмента текста и т. п.), при наличии цели использовать этот документ в измененном виде представляет собой способ подделки документа и квалифицируется по ст. 292 (служебный подлог) или по ст. 327 УК РФ (подделка, изготовление или сбыт поддельных документов), в зависимости от того, является ли субъект подделки государственным служащим или частным лицом;

– сокрытие документов – положение, когда документы оказались во владении виновного, не будучи им похищены (получены в силу служебного положения, переданы другим лицом, найдены и т. п.), и оставлены им у себя либо создание виновным условий для выхода документов из-под законного контроля со стороны учреждения, организации или лица, имеющего право на такой контроль или на распоряжение документами. В последнем случае документы могут и не изыматься из учреждения, организации и т. п., но виновный размещает их там таким образом, что собственник, владелец, пользователь, хранитель документов лишается возможности их обнаружить и распоряжаться ими.

Субъектом преступления, предусмотренного ч. 1 ст. 325 УК РФ, может быть любое физическое вменяемое лицо, достигшее шестнадцатилетнего возраста.

Субъективная сторона характеризуется прямым умыслом: виновный сознает, что похищает, уничтожает, повреждает или

скрывает официальный документ, и желает этого. Обязательным элементом субъективной стороны рассматриваемого преступления является мотив. Уголовная ответственность наступает, если похищение, уничтожение, повреждение, сокрытие официальных документов совершено из корыстной или личной заинтересованности.

Поощрительная норма, направленная на защиту государственной тайны

Ст. 275 УК РФ снабжена примечанием, согласно которому лицо, совершившее государственную измену (ст. 275 УК РФ) или шпионаж (ст. 276 УК РФ), «освобождается от уголовной ответственности, если оно добровольным и своевременным сообщением органам власти или иным способом способствовало предотвращению ущерба интересам Российской Федерации и если в его действиях не содержится иного состава преступления».

В этом примечании изложена так называемая поощрительная норма, которая позволяет лицу в случае его деятельного раскаяния после совершения деяний, образующих оконченное преступление, быть освобожденным от уголовной ответственности. Такой порядок установлен не для всех преступлений, а лишь для деяний, перечисленных в примечании, в том числе для государственной измены и шпионажа:

1. Данные преступления отличаются высокой степенью латентности, в связи с чем их полное раскрытие без деятельного раскаяния лиц, их совершивших, весьма затруднительно. Без деятельного раскаяния лица трудно, а иногда и невозможно, определить, какие конкретно сведения, составляющие государственную тайну, оно передало (выдало) иностранному государству, иностранной организации или их представителям, какое распространение получили эти сведения и как использовались.

2. Деятельное раскаяние лица позволяет свести к минимуму ущерб, причиненный совершением преступления, и предотвратить причинение дальнейшего вреда интересам внешней безопасности Российской Федерации: принять меры по изъятию переданных (выданных) субъектом материальных носителей государственной тайны; обеспечить безопасность лиц, информацию

о которых он сообщил «адресатам»; принять меры по дальнейшей зашифровке указанных сведений и по созданию у «адресатов» сомнений в достоверности полученных ими сведений и т. п.

3. Деятельное раскаяние во многих случаях позволяет выявить и в некоторой степени пресечь враждебную деятельность иностранных государств, иностранных организаций и их представителей против нашей страны, а также использовать полученную у раскаявшегося лица информацию в разведывательных, контрразведывательных и оперативно-разыскных целях, в том числе и для более эффективного обеспечения охраны государственной тайны.

Для освобождения от уголовной ответственности лица, совершившего государственную измену или шпионаж (согласно примечания к ст. 275 УК РФ), необходимо сочетание двух условий:

– способствование субъектом предотвращению дальнейшего ущерба интересам Российской Федерации путем добровольного и своевременного сообщения о содеянном органам власти или иным способом (например, путем изъятия у «адресата» полученных тем секретных сведений);

– отсутствие в действиях лица иного состава преступления.

При наличии этих условий лицо подлежит обязательному освобождению от уголовной ответственности.

2.7. Допуск предприятий, учреждений и организаций к проведению работ, связанных с использованием сведений, составляющих государственную тайну

Допуск предприятий, учреждений и организаций к 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, осуществляется путем получения ими (в порядке, устанавливаемом Правительством Российской Федерации) лицензий на проведение работ со сведениями соответствующей степени секретности.

Лицензия на проведение указанных работ выдается на основании результатов специальной экспертизы предприятия,

учреждения и организации и государственной аттестации их руководителей, ответственных за защиту сведений, составляющих государственную тайну (расходы по проведению относятся на счет предприятия, учреждения, организации, получающих лицензию).

Лицензия на проведение работ с использованием сведений, составляющих государственную тайну, выдается предприятию, учреждению, организации при:

– выполнении требований нормативных документов, утверждаемых Правительством Российской Федерации, по обеспечению защиты сведений, составляющих государственную тайну, в процессе выполнения работ, связанных с использованием указанных сведений;

– наличии в их структуре подразделений по защите государственной тайны и специально подготовленных сотрудников для работы по защите информации, количество и уровень квалификации которых достаточны для обеспечения защиты государственной тайны;

– наличии у них сертифицированных средств защиты информации.

2.8. Подготовка сотрудников для работы по защите информации, составляющей государственную тайну

Подготовка сотрудников для работы по защите информации, составляющей государственную тайну, осуществляется в соответствии с положениями Федерального закона от 29 декабря 2012 г. № 273-ФЗ «Об образовании в Российской Федерации», Законом Российской Федерации от 21 июля 1993 г. № 5485-1 «О государственной тайне», иных нормативных правовых актов в области защиты государственной тайны, нормативных правовых актов, регулирующих деятельность в области информационной безопасности, Приказа Министерства образования и науки РФ от 5 декабря 2013 г. № 1310 «Об утверждении Порядка разработки дополнительных профессиональных программ, содержащих сведения,

составляющие государственную тайну, и дополнительных профессиональных программ в области информационной безопасности».

Требования к дополнительным профессиональным программам, содержащие сведения, составляющие государственную тайну, и дополнительных профессиональных программ в области информационной безопасности определяются Межведомственной комиссией по защите государственной тайны, Федеральной службой безопасности Российской Федерации и Федеральной службой по техническому и экспортному контролю (обязательное согласование программ обучения).

Дополнительная профессиональная программа разрабатывается образовательной организацией по заказу органа государственной власти, организации или в инициативном порядке.

Содержание дополнительной профессиональной программы должно учитывать профессиональные стандарты, квалификационные требования, указанные в квалификационных справочниках по соответствующим должностям, профессиям и специальностям, или квалификационные требования к профессиональным знаниям и навыкам, необходимым для исполнения должностных обязанностей, связанных с использованием сведений, составляющих государственную тайну, или по вопросам информационной безопасности, которые устанавливаются в соответствии с федеральными законами и иными нормативными правовыми актами Российской Федерации о государственной службе.

В структуру дополнительной профессиональной программы должны быть включены: цель реализации программы; планируемые результаты обучения; требования к квалификации поступающего на обучение; форма обучения; учебный и (или) учебно-тематический план, программы дисциплин (модулей), условия реализации программы, формы аттестации, оценочные материалы и иные компоненты.

Условия реализации дополнительной профессиональной программы должны предусматривать особенности организации учебного процесса, в том числе ограничения, связанные с применением

исключительно электронного обучения и дистанционных образовательных технологий, порядок передачи дополнительной профессиональной программы другой образовательной организации, порядок внесения изменений в нее в соответствии с требованиями, установленными законодательными и иными нормативными правовыми актами Российской Федерации в области образования, защиты государственной тайны и информационной безопасности.

Особенности разработки дополнительных профессиональных программ, содержащих сведения, составляющие государственную тайну

К дополнительным профессиональным программам, содержащим сведения, составляющие государственную тайну, относятся дополнительные профессиональные программы (программы повышения квалификации и программы профессиональной переподготовки), при реализации которых предусматривается в период их освоения ознакомление слушателей со сведениями, составляющими государственную тайну, и (или) использование в учебных целях секретных образцов вооружения, военной и специальной техники, их комплектующих изделий, специальных материалов и веществ.

В дополнительной профессиональной программе или ее составной части, не содержащей сведения, составляющие государственную тайну, не допускаются ссылки на сведения, составляющие государственную тайну.

Дополнительная профессиональная программа должна включать перечень сведений, составляющих государственную тайну, используемых в учебном процессе с указанием распределения их по дисциплинам (модулям) и этапам учебного процесса.

Минимальный срок освоения программ повышения квалификации не может быть менее двадцати четырех часов, минимальный срок освоения программ профессиональной переподготовки – менее двухсот пятидесяти часов.

Для разработки дополнительной профессиональной программы, содержащей сведения, составляющие государственную тайну,

образовательная организация и организация должны иметь оформленную в установленном порядке лицензию на проведение работ с использованием сведений, составляющих государственную тайну.

Решение о самостоятельном инициировании разработки дополнительной профессиональной программы, содержащей сведения, составляющие государственную тайну, оформляется распорядительным актом руководителя образовательной организации и доводится образовательной организацией до сведения учредителя образовательной организации.

Руководитель образовательной организации – разработчика дополнительной профессиональной программы, несет ответственность за организацию выполнения требований по защите государственной тайны в процессе разработки дополнительной профессиональной программы.

Особенности разработки дополнительных профессиональных программ в области информационной безопасности

К дополнительным профессиональным программам в области информационной безопасности относятся программы повышения квалификации и программы профессиональной переподготовки, направленные на формирование и (или) совершенствование у слушателей компетенций в области информационной безопасности.

Минимальный срок освоения программ повышения квалификации в области информационной безопасности не может быть менее сорока часов, минимальный срок освоения программ профессиональной переподготовки в области информационной безопасности – менее трехсот шестидесяти часов.

Программы профессиональной переподготовки в области информационной безопасности утверждаются образовательной организацией по согласованию с федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, и (или) федеральным органом исполнительной власти в области обеспечения безопасности в соответствии с их компетенцией.

2.9. Квалификационные требования, указанные в квалификационных справочниках по должностям, профессиям и специальностям

Министерство здравоохранения и социального развития Российской Федерации приказом от 22.04.2009 № 205 ввело в действие Квалификационные характеристики должностей руководителей и специалистов по обеспечению безопасности информации в ключевых системах информационной инфраструктуры, противодействию техническим разведкам и технической защите информации, в которых определены должности руководителей и специалистов по этим направлениям деятельности, их должностные обязанности.

2.10. Порядок сертификации средств защиты информации

Постановлением Правительства Российской Федерации «О сертификации средств защиты информации» от 26.06.95 № 608 утверждено Положение о сертификации средств защиты информации.

Участниками сертификации средств защиты информации являются:

– федеральный орган по сертификации;

– центральный орган системы сертификации (создаваемый при необходимости) – орган, возглавляющий систему сертификации однородной продукции;

– органы по сертификации средств защиты информации – органы, проводящие сертификацию определенной продукции;

– испытательные лаборатории – лаборатории, проводящие сертификационные испытания (отдельные виды этих испытаний) определенной продукции;

– изготовители – продавцы, исполнители продукции.

Центральные органы системы сертификации, органы по сертификации средств защиты информации и испытательные лаборатории проводят аккредитацию на право проведения работ по сертификации, в ходе которой федеральные органы по сертификации определяют возможности выполнения этими органами

и лабораториями работ по сертификации средств защиты информации и оформляют официальное разрешение на право проведения указанных работ. Аккредитация проводится только при наличии у указанных органов и лабораторий лицензии на соответствующие виды деятельности.

Испытательные лаборатории проводят сертификационные испытания средств защиты информации и по их результатам оформляют заключения и протоколы, которые направляют в соответствующий орган по сертификации средств защиты информации и изготовителям.

Испытательные лаборатории несут ответственность за полноту испытаний средств защиты информации и достоверность их результатов.

Изготовители:

– производят (реализуют) средства защиты информации только при наличии сертификата;

– извещают орган по сертификации, проводивший сертификацию, об изменениях в технологии изготовления и конструкции (составе) сертифицированных средств защиты информации;

– маркируют сертифицированные средства защиты информации знаком соответствия в порядке, установленном для данной системы сертификации;

– указывают в сопроводительной технической документации сведения о сертификации и нормативных документах, которым средства защиты информации должны соответствовать, а также обеспечивают доведение этой информации до потребителя;

– применяют сертификат и знак соответствия, руководствуясь законодательством Российской Федерации и правилами, установленными для данной системы сертификации;

– обеспечивают соответствие средств защиты информации требованиям нормативных документов по защите информации;

– обеспечивают беспрепятственное выполнение своих полномочий должностными лицами органов, осуществляющих сертификацию, и контроль за сертифицированными средствами защиты информации;

– прекращают реализацию средств защиты информации при несоответствии их требованиям нормативных документов или по истечении срока действия сертификата, а также в случае приостановки действия сертификата или его отмены.

Изготовители должны иметь лицензию на соответствующий вид деятельности.

Срок действия сертификата не может превышать пяти лет.

Положением о сертификации средств защиты информации по требованиям безопасности информации, утвержденным приказом председателя Гостехкомиссии России от 27.10.1995 № 199, и Положением о системе сертификации средств защиты информации по требованиям безопасности для сведений, составляющих государственную тайну (система сертификации СЗИ-ГТ), введенным в действие приказом ФСБ России от 13 ноября 1999 г. № 564, установлены основные принципы, организационная структура системы сертификации СЗИ-ГТ, порядок проведения сертификации этих средств, порядок регистрации сертифицированных средств, а также порядок проведения инспекционного контроля за сертифицированными средствами. Государственный контроль и надзор за соблюдением заявителями, испытательными центрами (лабораториями) и органами по сертификации правил обязательной сертификации осуществляет ФСБ России в порядке, установленном законодательством Российской Федерации.

Органы по сертификации системы сертификации СЗИ-ГТ проводят обязательную сертификацию средств защиты информации, используемых при работе со сведениями, составляющими государственную тайну, в том числе иностранного производства. Номенклатура СЗИ-ГТ разрабатывается ФСБ России на основании видов средств защиты информации, подлежащих сертификации в системе сертификации СЗИ-ГТ, и утверждается по согласованию с Межведомственной комиссией по защите государственной тайны.

По правилам системы сертификации СЗИ-ГТ по инициативе разработчика, изготовителя или потребителя может также проводиться добровольная сертификация средств защиты информации, не предназначенных для работы со сведениями, составляющими государственную тайну.

Сертификация СЗИ-ГТ осуществляется аккредитованными органами по сертификации, а испытания проводятся в аккредитованных испытательных центрах (лабораториях).

Порядок проведения сертификации включает следующие действия:

– подачу и рассмотрение заявки на сертификацию СЗИ-ГТ;

– испытания сертифицируемых СЗИ-ГТ и анализ состояния их производства;

– экспертизу результатов испытаний, оформление, регистрацию и выдачу сертификата соответствия и лицензии на право применения знака соответствия;

– осуществление инспекционного контроля за соблюдением правил обязательной сертификации и за сертифицированными СЗИ-ГТ, информирование о результатах сертификации СЗИ-ГТ;

– рассмотрение апелляций.

С 1 августа 2018 года вступило в силу новое Положение о системе сертификации средств защиты информации, утвержденное приказом ФСТЭК России № 55 от 3 апреля 2018 г.

В основном оно рассчитано на разработчиков СЗИ. Но есть некоторые новые нюансы, интересные пользователям и лицензиатам: теперь официально разрешено применять СЗИ после окончания срока действия сертификата ФСТЭК (сертификат был, но срок закончился), до того момента, пока производитель оказывает техническую поддержку СЗИ или ФСТЭК явно не отзовет сертификат.

На сайте ФСТЭК России имеется перечень органов по аттестации, реестр аккредитованных ФСТЭК России органов по сертификации и испытательных лабораторий и государственный реестр сертифицированных средств защиты информации.

2.11. Финансирование мероприятий по защитегосударственной тайны

В соответствии с Законом Российской Федерации от 21.07.1993 № 5485-1 «О государственной тайне» финансирование деятельности органов государственной власти, бюджетных предприятий, учреждений и организаций и их структурных подразделений по

защите государственной тайны осуществляется за счет средств соответствующих бюджетов, а остальных предприятий, учреждений и организаций – *за счет средств, получаемых от их основной деятельности при выполнении работ, связанных с использованием сведений, составляющих государственную тайну.*

Средства на финансирование государственных программ в области защиты государственной тайны предусматриваются в федеральном бюджете Российской Федерации отдельной строкой.

Контроль за расходованием финансовых средств, выделяемых на проведение мероприятий по защите государственной тайны, осуществляется руководителями органов государственной власти, предприятий, учреждений и организаций, заказчиками работ, а также специально уполномоченными на то представителями Министерства финансов Российской Федерации. Если осуществление этого контроля связано с доступом к сведениям, составляющим государственную тайну, то перечисленные лица должны иметь допуск к сведениям соответствующей степени секретности.

В договорах на проведение совместных и других работ, заключаемых в установленном законом порядке, предусматриваются условия финансирования работ (услуг) по защите сведений, составляющих государственную тайну.

Расходы по проведению мероприятий на получение лицензий по проведению работ, связанных с использованием сведений, составляющих государственную тайну, создание средств защиты информации, а также осуществление мероприятий и (или) оказание услуг по защите государственной тайны относятся на счет предприятия, учреждения, организации, получающих лицензию.

В соответствии с Положением о государственной системе защиты информации в Российской Федерации от иностранных технических разведок и от ее утечки по техническим каналам, утвержденным Постановлением Совета Министров – Правительства Российской Федерации от 15.09.1993 № 912-51:

– финансирование мероприятий по защите информации, содержащей сведения, отнесенные к государственной или служебной тайне, а также подразделений по защите информации

в органах государственной власти и на бюджетных предприятиях предусматривается в сметах расходов на их содержание;

– создание технических средств защиты информации, не требующее капитальных вложений, осуществляется в пределах средств, выделяемых заказчиком на научно-исследовательские и опытно-конструкторские работы, связанные с разработкой продукции;

– расходы по разработке технических средств защиты информации включаются в стоимость разработки образца продукции;

– создание технических средств защиты информации, требующее капитальных вложений, осуществляется в пределах средств, выделяемых заказчиком на строительство (реконструкцию) сооружений или объектов.

2.12. Контроль и надзор за обеспечением защиты государственной тайны

Один – тайна, два – полтайны, три – нет тайны.

Поговорка

В соответствии с Законом Российской Федерации от 21.07.1993 № 5485-1 «О государственной тайне» Контроль за обеспечением защиты государственной тайны осуществляют Президент Российской Федерации, Правительство Российской Федерации в пределах полномочий, определяемых Конституцией Российской Федерации, федеральными конституционными законами и федеральными законами.

Федеральный государственный контроль за обеспечением защиты государственной тайны осуществляется уполномоченными федеральными органами исполнительной власти (далее – органы государственного контроля) согласно их компетенции в порядке, установленном Правительством Российской Федерации.

К отношениям, связанным с осуществлением федерального государственного контроля за обеспечением защиты государственной

тайны, организацией и проведением проверок на предприятиях, в учреждениях и организациях (далее для целей настоящей статьи – юридические лица), применяются положения Федерального закона от 26.12.2008 № 294-ФЗ «О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля» с учетом особенностей организации и проведения проверок, установленных ч. 3–9 настоящей статьи.

О проведении плановой проверки юридическое лицо уведомляется не позднее трех рабочих дней до ее начала путем направления органом государственного контроля письменного уведомления.

Основанием для проведения внеплановой выездной проверки является:

– истечение срока исполнения юридическим лицом выданного органом государственного контроля предписания об устранении выявленного нарушения требований законодательства Российской Федерации в области защиты государственной тайны;

– поступление в органы государственного контроля информации, указывающей на признаки нарушения требований законодательства Российской Федерации о государственной тайне;

– наличие предписания (приказа, распоряжения или иного распорядительного документа) руководителя (уполномоченного им должностного лица) органа государственного контроля о проведении внеплановой проверки, изданного в соответствии с поручением Президента Российской Федерации или Правительства Российской Федерации либо на основании требования прокурора о проведении внеплановой проверки в рамках надзора за исполнением законов по поступившим в органы прокуратуры материалам и обращениям.

Срок проведения проверки составляет не более тридцати рабочих дней со дня начала ее проведения.

В исключительных случаях, связанных с необходимостью проведения сложных и (или) длительных исследований, испытаний, специальных экспертиз и расследований на основании мотивированных предложений должностных лиц органа государственного

контроля, проводящих проверку, срок проведения проверки может быть продлен руководителем органа государственного контроля (уполномоченным им должностным лицом), но не более чем на двадцать рабочих дней.

Выездная проверка юридических лиц проводится на основании предписания (приказа, распоряжения или иного распорядительного документа), подписанного руководителем (уполномоченным им должностным лицом) органа государственного контроля.

Внеплановая выездная проверка проводится без предварительного уведомления.

Информация об организации проверок, проводимых органами государственного контроля, в том числе о планировании, проведении и результатах таких проверок, в органы прокуратуры не направляется.

Межведомственный контроль за обеспечением защиты государственной тайны в органах государственной власти осуществляют 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, на которые эта функция возложена законодательством Российской Федерации.

Органы государственной власти, наделенные в соответствии с настоящим Законом полномочиями по распоряжению сведениями, составляющими государственную тайну, обязаны контролировать эффективность защиты этих сведений во всех подчиненных и подведомственных им органах государственной власти, на предприятиях, в учреждениях и организациях, осуществляющих работу с ними.

Контроль за обеспечением защиты государственной тайны в Администрации Президента Российской Федерации, в аппаратах

палат Федерального Собрания, Правительства Российской Федерации организуется их руководителями.

Контроль за обеспечением защиты государственной тайны в судебных органах и органах прокуратуры организуется руководителями этих органов.

Надзор за соблюдением законодательства при обеспечении защиты государственной тайны и законностью принимаемых при этом решений осуществляют Генеральный прокурор Российской Федерации и подчиненные ему прокуроры.

Доступ лиц, осуществляющих прокурорский надзор, к сведениям, составляющим государственную тайну, осуществляется в соответствии со ст. 25 Закона о государственной тайне.

Правила организации и осуществления федерального государственного контроля за обеспечением защиты государственной тайны утверждены постановлением Правительства Российской Федерации от 22.11.2012 № 1205.

Органы государственного контроля проводят проверки выполнения юридическими лицами требований законодательства о государственной тайне и осуществления следующих мер по обеспечению сохранности сведений, составляющих государственную тайну:

– создание и организация деятельности структурных подразделений по защите государственной тайны;

– допуск должностных лиц и граждан к государственной тайне;

– выполнение работниками, допущенными к сведениям, составляющим государственную тайну, возложенных на них обязанностей по их защите и соблюдение ими соответствующих ограничений и запретов;

– засекречивание сведений, составляющих государственную тайну;

– организация и осуществление пропускного режима;

– организация и проведение совещаний по секретным вопросам;

– обеспечение режима секретности;

– организация выезда работников, осведомленных в сведениях, составляющих государственную тайну, за границу;

– организация и осуществление приема иностранных граждан;

– передача сведений, составляющих государственную тайну, и их носителей другим организациям (включая международные) и государствам;

– подготовка к работе с носителями сведений, составляющих государственную тайну, в период мобилизации и в военное время;

– оборудование и эксплуатация режимных помещений и хранилищ носителей сведений, составляющих государственную тайну;

– обращение с носителями сведений, составляющих государственную тайну;

– защита секретной информации, обрабатываемой с использованием средств вычислительной техники;

– прием, сдача носителей сведений, составляющих государственную тайну, при смене руководителя режимно-секретного подразделения или подразделения секретного делопроизводства, при реорганизации или ликвидации организации;

– организация и ведение секретного делопроизводства;

– организация и осуществление противодействия иностранным техническим разведкам;

– организация и осуществление технической защиты информации;

– организация и осуществление защиты информации, содержащей сведения, составляющие государственную тайну, с использованием шифровальных (криптографических) средств;

– осуществление контроля за обеспечением защиты государственной тайны;

– организация и проведение служебных расследований (служебных проверок) по фактам нарушения режима секретности и обязательных требований в области противодействия иностранным техническим разведкам, технической защиты информации и защиты информации с использованием шифровальных (криптографических) средств.

В соответствии с постановлением Правительства Российской Федерации от 16.05.2011 № 373 «О разработке и утверждении административных регламентов исполнения государственных

функций и административных регламентов предоставления государственных услуг» утвержден Административный регламент Федеральной службы безопасности Российской Федерации по исполнению государственной функции по осуществлению федерального государственного контроля за обеспечением защиты государственной тайны приказом ФСБ России от 05.03.2015 № 152.

Предметом федерального государственного контроля является соблюдение предприятиями, учреждениями и организациями, осуществляющими деятельность, связанную с использованием сведений, составляющих государственную тайну, их руководителями, должностными и иными лицами требований, установленных Законом Российской Федерации от 21.07.1993 № 5485-1 «О государственной тайне», другими федеральными законами и принятыми на их основе иными нормативными правовыми актами.

Права и обязанности должностных лиц при исполнении государственной функции

При исполнении государственной функции по осуществлению федерального государственного контроля за обеспечением защиты государственной тайны должностные лица, уполномоченные осуществлять федеральный государственный контроль за обеспечением защиты государственной тайны, в пределах своей компетенции имеют право:

1) доступа к документам, журналам (карточкам) учета и другим материалам и изделиям, местам их хранения, а также к техническим средствам, автоматизированным системам и информации, хранящейся на машинных носителях информации, относящимся к проверке (при проведении выездной проверки);

2) осуществлять иные полномочия, предоставленные Федеральным законом от 03.04.1995 № 40-ФЗ «О федеральной службе безопасности».

Должностные лица органа государственного контроля при исполнении государственной функции по осуществлению федерального государственного контроля за обеспечением защиты государственной тайны обязаны:

1) своевременно и в полной мере исполнять предоставленные в соответствии с законодательством Российской Федерации

полномочия по предупреждению, выявлению и пресечению нарушений требований законодательства о государственной тайне;

2) соблюдать законодательство Российской Федерации, права и законные интересы организаций, проверка которых проводится;

3) проводить проверки в соответствии с их назначением: выездную проверку – на основании предписания на проверку, предусмотренного ч. 7 ст. 30.1 Закона Российской Федерации от 21.07.1993 № 5485-1 «О государственной тайне», а документарную – на основании распоряжения или приказа руководителя, заместителя руководителя органа государственного контроля о проведении проверки;

4) проводить проверку только во время исполнения служебных обязанностей, выездную проверку – при предъявлении служебных удостоверений и предписания о проведении проверки;

5) не препятствовать руководителю, иному должностному лицу или уполномоченному представителю организации, имеющему допуск к государственной тайне по соответствующей форме и непосредственное отношение к предмету проверки, присутствовать при проведении проверки и давать разъяснения по вопросам, относящимся к ее предмету;

6) предоставлять руководителю, иному должностному лицу или уполномоченному представителю организации, присутствующему при проведении проверки и имеющему допуск к государственной тайне по соответствующей форме, информацию и документы, относящиеся к предмету проверки, за исключением информации, свободное распространение которой запрещено или ограничено в соответствии с законодательством Российской Федерации;

7) знакомить руководителя, иное должностное лицо или уполномоченного представителя организации, имеющего допуск к государственной тайне по соответствующей форме и непосредственное отношение к предмету проверки, с результатами проверки;

8) учитывать при определении мер, принимаемых по фактам выявленных нарушений, соответствие указанных мер тяжести нарушений, а также не допускать необоснованное ограничение прав и законных интересов организации;

9) доказывать обоснованность своих действий при их обжаловании организациями в порядке, установленном законодательством Российской Федерации;

10) соблюдать установленные законодательством Российской Федерации сроки проведения проверки;

11) не требовать от организаций документы и иные сведения, представление которых не предусмотрено законодательством Российской Федерации;

12) перед началом проведения выездной проверки по просьбе руководителя, иного должностного лица или уполномоченного представителя организации ознакомить их с положениями настоящего Административного регламента;

13) осуществлять запись о проведенной проверке в журнале учета проверок.

Права и обязанности лиц, в отношении которых осуществляются мероприятия по контролю

Руководитель, иное должностное лицо или уполномоченный представитель организации, имеющий допуск к государственной тайне по соответствующей форме и непосредственное отношение к предмету проверки, имеет право:

1) непосредственно присутствовать при проведении выездной проверки, давать объяснения по вопросам, относящимся к предмету проверки;

2) получать от органа государственного контроля и его должностных лиц информацию, которая относится к предмету проверки и предоставление которой предусмотрено законодательством Российской Федерации;

3) знакомиться с результатами проверки и указывать в акте проверки о своем ознакомлении с результатами проверки, согласии или несогласии с ними, а также с отдельными действиями должностных лиц органа государственного контроля;

4) обжаловать действия (бездействие) должностных лиц органа государственного контроля, повлекшие за собой нарушение прав или законных интересов организации при проведении проверки, в административном и (или) судебном порядке в соответствии с законодательством Российской Федерации;

5) привлекать Уполномоченного при Президенте Российской Федерации по защите прав предпринимателей либо уполномоченного по защите прав предпринимателей в субъекте Российской Федерации к участию в проверке.

Руководитель, иное должностное лицо или уполномоченный представитель организации обязан:

1) присутствовать и обеспечить присутствие должностных лиц, ответственных за организацию и проведение мероприятий по выполнению требований законодательства о государственной тайне;

2) предоставить должностным лицам органа государственного контроля, проводящим выездную проверку, возможность ознакомиться с документами, связанными с целями, задачами и предметом выездной проверки, в случае если выездной проверке не предшествовало проведение документарной проверки, а также обеспечить доступ проводящих выездную проверку должностных лиц и участвующих в выездной проверке представителей иных государственных органов и организаций на территорию, в используемые организацией при осуществлении деятельности здания, строения, сооружения, помещения, к используемым организацией оборудованию и подобным объектам, относящимся к предмету проверки.

Описание результата исполнения государственной функции

Результатом исполнения государственной функции по осуществлению федерального государственного контроля за обеспечением защиты государственной тайны является получение объективной информации о соблюдении организацией требований законодательства о государственной тайне, а также выявление, пресечение и предупреждение нарушений требований законодательства о государственной тайне (рис. 2.13).

Исполнение государственной функции завершается составлением акта проверки.

Информирование о порядке исполнения государственной функции по осуществлению федерального государственного контроля за обеспечением защиты государственной тайны осуществляется:

Рис. 2.13. Направления проверок обеспечения защиты сведений, отнесенных к государственной тайне

1) посредством размещения информации о порядке исполнения государственной функции на официальном сайте ФСБ России в информационно-телекоммуникационной сети Интернет: www.fsb.ru;

2) посредством размещения информации о порядке исполнения государственной функции в федеральной государственной информационной системе «Единый портал государственных и муниципальных услуг (функций)»: www.gosuslugi.ru;

3) посредством использования средств телефонной связи, электронной почты, при устном или письменном обращении граждан.

Плата за осуществление мероприятий по контролю за обеспечением защиты государственной тайны с организации, в отношении которой проводятся указанные мероприятия, не взимается.

Срок исполнения государственной функции включает в себя срок проведения проверки и срок подготовки акта проверки.

Срок проведения проверки составляет не более чем тридцать рабочих дней со дня начала ее проведения.

В исключительных случаях, связанных с необходимостью проведения сложных и (или) длительных исследований, испытаний, специальных экспертиз и расследований на основании мотивированных предложений должностных лиц органа государственного контроля, проводящих проверку, срок проведения проверки может быть продлен руководителем органа государственного контроля (уполномоченным им должностным лицом), но не более чем на двадцать рабочих дней.

Акт проверки оформляется непосредственно после ее завершения.

В рамках федерального государственного контроля за обеспечением защиты государственной тайны органами безопасности проводятся *плановые и внеплановые выездные и документарные проверки*.

Плановая проверка проводится на основании ежегодного плана проведения плановых проверок не чаще одного раза в три года.

Выездная проверка проводится на основании предписания о проведении проверки, оформленного на бланке органа государственного контроля и подписанного уполномоченным должностным лицом органа государственного контроля.

Выездная проверка (как плановая, так и внеплановая) проводится по месту нахождения организации и (или) по месту фактического осуществления организацией деятельности, связанной с использованием сведений, составляющих государственную тайну.

Документарная проверка (как плановая, так и внеплановая) проводится по месту нахождения органа государственного контроля.

В процессе проведения документарной проверки должностными лицами органа государственного контроля в первую очередь рассматриваются документы организации, имеющиеся в распоряжении органа государственного контроля, в том числе акты предыдущих проверок, материалы рассмотрения дел об административных правонарушениях и иные документы о результатах

проверочных мероприятий, осуществленных в отношении проверяемой организации.

Текущий контроль за исполнением государственной функции по осуществлению федерального государственного контроля за обеспечением защиты государственной тайны осуществляется уполномоченными должностными лицами органа государственного контроля.

Текущий контроль осуществляется постоянно.

Контроль за полнотой и качеством исполнения государственной функции по осуществлению федерального государственного

Рис. 2.14. Блок-схема исполнения государственной функции

контроля за обеспечением защиты государственной тайны территориальными органами безопасности и органами безопасности в войсках осуществляет Центр по лицензированию, сертификации и защите государственной тайны ФСБ России и Департамент военной контрразведки ФСБ России соответственно, а также Инспекторское управление Контрольной службы ФСБ России.

Контроль за полнотой и качеством исполнения государственной функции по осуществлению федерального государственного контроля за обеспечением защиты государственной тайны Центром по лицензированию, сертификации и защите государственной тайны ФСБ России и Департаментом военной контрразведки ФСБ России осуществляет Инспекторское управление Контрольной службы ФСБ России.

Порядок и периодичность осуществления плановых и внеплановых проверок полноты и качества исполнения государственной функции устанавливаются правовыми актами ФСБ России, планами работы органов безопасности, подразделений ФСБ России, а также решениями руководства ФСБ России.

Блок-схема исполнения государственной функции представлена на рис. 2.14.

2.13. Лицензирование 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

Порядок лицензирования определяется Положением 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, утвержденным постановлением Правительства РФ от 15.04.1995 № 333, а также Административным регламентом Федеральной

службы безопасности Российской Федерации по исполнению государственной функции по лицензированию 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, введенным приказом ФСБ России от 27.02.2009 № 75.

Лицензия является официальным документом, который разрешает осуществление на определенных условиях конкретного вида деятельности в течение установленного срока. Лицензия действительна на всей территории Российской Федерации, а также в учреждениях Российской Федерации, находящихся за границей.

Органами, уполномоченными на ведение лицензионной деятельности, являются:

– по допуску предприятий к проведению работ, связанных с использованием сведений, составляющих государственную тайну, – Федеральная служба безопасности Российской Федерации и ее территориальные органы (на территории Российской Федерации), Служба внешней разведки Российской Федерации (за рубежом);

– на право проведения работ, связанных с созданием средств защиты информации, – Федеральная служба по техническому и экспортному контролю, Служба внешней разведки Российской Федерации, Министерство обороны Российской Федерации, Федеральная служба безопасности Российской Федерации (в пределах их компетенции);

– на право осуществления мероприятий и (или) оказания услуг в области защиты государственной тайны – Федеральная служба безопасности Российской Федерации и ее территориальные органы, Федеральная служба по техническому и экспортному контролю, Служба внешней разведки Российской Федерации (в пределах их компетенции).

Лицензирование деятельности предприятий Федеральной службы безопасности Российской Федерации, Министерства обороны Российской Федерации, Федеральной пограничной

Рис. 2.15. Система лицензирования в области защиты информации, составляющей государственную тайну

службы Российской Федерации, Службы внешней разведки Российской Федерации, Федеральной службы по техническому и экспортному контролю по допуску к проведению работ, связанных с использованием сведений, составляющих государственную тайну, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны, осуществляется руководителями министерств и ведомств Российской Федерации, которым подчинены указанные предприятия (рис. 2.15).

На орган, уполномоченный на ведение лицензионной деятельности, возлагается:

– организация лицензирования деятельности предприятий;

– организация и проведение специальных экспертиз предприятий;

– рассмотрение заявлений предприятий о выдаче лицензий;

– принятие решений о выдаче или об отказе в выдаче лицензий;

– выдача лицензий;

– принятие решений о приостановлении действия лицензии или о ее аннулировании;

– разработка нормативно-методических документов по вопросам лицензирования;

– привлечение в случае необходимости представителей министерств и ведомств Российской Федерации для проведения специальных экспертиз;

– ведение реестра выданных, приостановленных и аннулированных лицензий.

Работа органов, уполномоченных на ведение лицензионной деятельности, координируется Межведомственной комиссией по защите государственной тайны.

Для получения лицензии заявитель представляет в соответствующий орган, уполномоченный на ведение лицензионной деятельности, следующие документы:

а) заявление о выдаче лицензии с указанием:

– наименования, организационно-правовой формы и местонахождения предприятия;

– идентификационного номера налогоплательщика;

– даты уплаты предприятием государственной пошлины за предоставление лицензии;

– сведений о наличии допуска к государственной тайне у руководителя предприятия;

– адресов мест осуществления лицензируемого вида деятельности;

– реквизитов правоустанавливающих документов на объекты недвижимости, необходимые для осуществления заявленного вида деятельности на срок действия лицензии, права на которые зарегистрированы в Едином государственном реестре прав на недвижимое имущество и сделок с ним;

– вида деятельности, на осуществление которого должна быть выдана лицензия;

– срока действия лицензии;

– подтвержденной в установленном порядке степени секретности сведений, составляющих государственную тайну, с которыми заявитель предполагает проводить работы;

– формы предоставления лицензии (на бумажном носителе или в электронной форме (в форме электронного документа, подписанного электронной подписью));

б) копии учредительных документов юридического лица;

в) копии правоустанавливающих документов на объекты недвижимости, необходимые для осуществления заявленного вида деятельности на срок действия лицензии, права на которые не зарегистрированы в Едином государственном реестре прав на недвижимое имущество и сделок с ним;

г) копия договора об оказании услуг (в случае использования заявителем услуг структурного подразделения по защите государственной тайны другой организации).

Заявитель вправе представить документы для получения лицензии на бумажных носителях или в электронной форме (в форме электронных документов, подписанных электронной подписью).

Заявитель несет ответственность за достоверность представляемых им сведений.

Все документы, представленные для получения лицензии, регистрируются органом, уполномоченным на ведение лицензионной деятельности.

При проведении проверки сведений, содержащихся в заявлении и прилагаемых к нему документах, лицензирующий орган запрашивает необходимые сведения, находящиеся в распоряжении органов, предоставляющих государственные услуги, органов, предоставляющих муниципальные услуги, иных государственных органов, органов местного самоуправления либо подведомственных государственным органам или органам местного самоуправления организаций, в порядке, установленном Федеральным законом «Об организации предоставления государственных и муниципальных услуг».

Орган, уполномоченный на ведение лицензионной деятельности, принимает решение о выдаче или об отказе в выдаче лицензии в течение тридцати дней со дня получения заявления со всеми необходимыми документами.

В случае необходимости проведения дополнительной экспертизы предприятия решение принимается в пятнадцатидневный срок после получения заключения экспертизы, но не позднее чем через шестьдесят дней со дня подачи заявления о выдаче лицензии и необходимых для этого документов.

В зависимости от сложности и объема подлежащих специальной экспертизе материалов руководитель органа, уполномоченного на ведение лицензионной деятельности, может продлить срок принятия решения о выдаче или об отказе в выдаче лицензии до тридцати дней:

– прием и регистрация заявления и документов – один день;

– рассмотрение заявления и документов – четыре дня;

– проведение специальной экспертизы предприятия и государственной аттестации его руководителя, ответственного за защиту сведений, составляющих государственную тайну, – пятнадцать дней;

– подготовка решения органа, уполномоченного на ведение лицензионной деятельности, – семь дней;

– уведомление заявителя о решении органа, уполномоченного на ведение лицензионной деятельности, – три дня.

Лицензия считается возобновленной после принятия органом, уполномоченным на ведение лицензионной деятельности, соответствующего решения, о котором не позднее чем в трехдневный срок с момента принятия он оповещает лицензиата.

Лицензии выдаются на основании результатов специальных экспертиз предприятий и государственной аттестации их руководителей, ответственных за защиту сведений, составляющих государственную тайну (далее именуются – руководители предприятий), и при выполнении следующих условий:

– соблюдение требований законодательных и иных нормативных актов Российской Федерации по обеспечению защиты сведений, составляющих государственную тайну, в процессе выполнения работ, связанных с использованием указанных сведений;

– наличие в структуре предприятия подразделения по защите государственной тайны и необходимого числа специально подготовленных сотрудников для работы по защите информации,

уровень квалификации которых достаточен для обеспечения защиты государственной тайны;

– наличие на предприятии средств защиты информации, имеющих сертификат, удостоверяющий их соответствие требованиям по защите сведений соответствующей степени секретности.

В лицензии указываются:

– наименование органа, выдавшего лицензию;

– наименование, место нахождения предприятия, адреса мест осуществления лицензируемого вида деятельности (при необходимости), в том числе адреса мест осуществления лицензируемого вида деятельности подразделениями предприятия;

– идентификационный номер налогоплательщика;

– вид деятельности, на осуществление которого выдана лицензия;

– условия осуществления вида деятельности, на который выдана лицензия;

– степень секретности разрешенных к использованию сведений, составляющих государственную тайну, для лицензии на проведение работ, связанных с использованием сведений, составляющих государственную тайну;

– срок действия лицензии;

– регистрационный номер и дата выдачи лицензии.

Срок действия лицензии устанавливается в зависимости от специфики вида деятельности, но не более чем на пять лет. По просьбе заявителя лицензия может выдаваться на срок менее пяти лет. Срок действия лицензии, выданной предприятию, не может превышать срока действия лицензии предприятия, структурное подразделение по защите государственной тайны которого оказывает услуги по защите государственной тайны.

Продление срока действия лицензии производится в порядке, установленном для ее получения.

Предприятие может иметь несколько лицензий.

В случае если лицензируемый вид деятельности осуществляется подразделениями лицензиата по нескольким адресам, предоставление таким подразделениям права осуществлять заявленный

вид деятельности производится с учетом результатов специальной экспертизы этих подразделений и государственной аттестации их руководителей.

Лицензия оформляется на бланке, имеющем степень защиты на уровне степени защиты ценной бумаги. Бланки лицензий являются документами строгой отчетности, имеют учетную серию и номер. Приобретение, учет и хранение таких бланков возлагается на органы, уполномоченные на ведение лицензионной деятельности. Лицензия может иметь приложения, являющиеся ее неотъемлемой частью (о чем в ней делается соответствующая запись) и содержащие информацию о лицензиате.

Лицензия может быть оформлена на нескольких имеющих индивидуальные учетные и регистрационные номера бланках для подразделений лицензиата, расположенных вне места его нахождения. Срок действия оформленной таким образом лицензии не может превышать срок действия лицензии, выданной предприятию, в структуру которого входят указанные подразделения. Срок действия лицензии по допуску предприятий к проведению работ, связанных с использованием сведений, составляющих государственную тайну, выдаваемой для территориального учреждения Центрального банка Российской Федерации, устанавливается независимо от срока действия лицензии, выданной Центральному банку Российской Федерации по месту осуществления его деятельности.

Лицензия подписывается руководителем органа, уполномоченного на ведение лицензионной деятельности, либо лицом, им уполномоченным, и заверяется печатью этого органа. Копия лицензии хранится в органе, уполномоченном на ведение лицензионной деятельности.

В случае изменений условий ведения лицензируемого вида деятельности, изменения степени секретности сведений, с которыми осуществляется (предполагается осуществлять) деятельность, а также в отношении которых лицензиат предполагает проводить мероприятия и (или) оказывать услуги, смены организационно-правовой формы или реорганизации лицензиата,

изменения его наименования, места нахождения, адресов мест осуществления лицензируемого вида деятельности лицензиат или его правопреемник обязаны в пятнадцатидневный срок подать в орган, уполномоченный на ведение лицензионной деятельности, заявление о переоформлении лицензии в связи с изменением условий деятельности с приложением документов, подтверждающих соответствующие изменения. В указанных случаях орган, уполномоченный на ведение лицензионной деятельности, по результатам рассмотрения заявления и проведения проверки соответствия предприятия лицензионным требованиям и условиям принимает решение о необходимости проведения специальной экспертизы и уведомляет о своем решении заявителя. В случае принятия решения о необходимости проведения специальной экспертизы выдача лицензии производится с учетом ее результатов.

В случае утраты лицензии предприятие имеет право на получение дубликата лицензии, который выдается на основании поданного в трехдневный срок со дня установления факта утраты заявления в письменной форме.

До переоформления лицензии (получения дубликата лицензии) предприятие осуществляет деятельность на основании ранее выданной лицензии, но не более шестидесяти дней.

Орган, уполномоченный на ведение лицензионной деятельности, вправе отказать в выдаче лицензии. Письменное уведомление об отказе в выдаче лицензии с указанием причин отказа направляется заявителю в трехдневный срок после принятия соответствующего решения.

Основанием для отказа в выдаче лицензии является:

– наличие в документах, представленных заявителем, недостоверной или искаженной информации;

– отрицательное заключение экспертизы, установившей несоответствие необходимым для осуществления заявленного вида деятельности условиям, указанным в п. 7 настоящего Положения;

– отрицательное заключение по результатам государственной аттестации руководителя предприятия.

Специальная экспертиза предприятия проводится путем проверки выполнения требований нормативно-методических документов по режиму секретности, противодействию иностранным техническим разведкам и защите информации от утечки по техническим каналам, а также соблюдения других условий, необходимых для получения лицензии.

Государственными органами, ответственными за организацию и проведение специальных экспертиз предприятий, являются Федеральная служба безопасности Российской Федерации, Федеральная служба по техническому и экспортному контролю, Служба внешней разведки Российской Федерации, Министерство обороны Российской Федерации, другие министерства и ведомства Российской Федерации и Государственная корпорация по атомной энергии «Росатом», руководители которых наделены полномочиями по отнесению к государственной тайне сведений в отношении подведомственных им предприятий.

Организация и порядок проведения специальных экспертиз предприятий определяются инструкциями, которые разрабатываются указанными государственными органами и согласовываются с Межведомственной комиссией.

Для проведения специальных экспертиз эти государственные органы могут создавать аттестационные центры, а также привлекать в установленном порядке предприятия, которые получают лицензии на проведение работ, связанных с использованием сведений, составляющих государственную тайну, а также на осуществление мероприятий и (или) оказание услуг по защите государственной тайны. Требования к данным предприятиям (аттестационным центрам) определяются органами, уполномоченными на ведение лицензионной деятельности.

Специальные экспертизы предприятий (аттестационных центров) проводят Федеральная служба безопасности Российской Федерации, Федеральная служба по техническому и экспортному контролю, Служба внешней разведки Российской Федерации, Министерство обороны Российской Федерации и их органы на местах (в пределах их компетенции).

Специальные экспертизы проводятся на основе договора между предприятием и органом, проводящим специальную экспертизу. Расходы по проведению специальных экспертиз относятся на счет предприятия.

Государственная аттестация руководителей предприятий организуется органами, уполномоченными на ведение лицензионной деятельности, а также министерствами и ведомствами Российской Федерации и Государственной корпорацией по атомной энергии «Росатом», руководители которых наделены полномочиями по отнесению к государственной тайне сведений в отношении подведомственных им предприятий.

Методические рекомендации по организации и проведению государственной аттестации руководителей предприятий разрабатываются Межведомственной комиссией.

Расходы по государственной аттестации руководителей предприятий относятся на счет предприятий.

Руководители предприятий, имеющие документ об образовании и (или) о квалификации, выданный организацией, осуществляющей образовательную деятельность, включенной в перечень, определяемый Межведомственной комиссией, считаются прошедшими государственную аттестацию, если со времени окончания организации, осуществляющей образовательную деятельность, прошло не более пяти лет.

Органы, уполномоченные на ведение лицензионной деятельности, приостанавливают действие лицензии или аннулируют ее в случае:

– предоставления лицензиатом соответствующего заявления;

– обнаружения недостоверных данных в документах, представленных для получения лицензии;

– нарушения лицензиатом условий действия лицензии;

– невыполнения лицензиатом предписаний или распоряжений государственных органов или приостановления этими государственными органами деятельности предприятия в соответствии с законодательством Российской Федерации;

– ликвидации предприятия.

Решение о приостановлении, возобновлении и аннулировании лицензии принимается органом, выдавшим лицензию.

Уведомление о приостановлении действия лицензии или об аннулировании лицензии орган, уполномоченный на ведение лицензионной деятельности, направляет лицензиату в письменной форме не позднее чем через три дня со дня принятия такого решения.

Лицензиат, получивший решение органа, уполномоченного на ведение лицензионной деятельности, о приостановлении действия лицензии или об аннулировании лицензии, обязан в десятидневный срок возвратить лицензию и уведомить о приостановлении действия (аннулировании) лицензии всех заинтересованных лиц. До принятия решения о возобновлении действия лицензии она хранится в органе, уполномоченном на ведение лицензионной деятельности.

Орган, уполномоченный на ведение лицензионной деятельности, устанавливает срок устранения лицензиатом обстоятельств, повлекших за собой приостановление действия лицензии. Указанный срок не может превышать шести месяцев.

В случае устранения обстоятельств, повлекших приостановление действия лицензии, ее действие может быть возобновлено. Лицензия считается возобновленной после принятия органом, уполномоченным на ведение лицензионной деятельности, соответствующего решения, о котором он в трехдневный срок со дня принятия решения оповещает лицензиата и возвращает ему лицензию, содержащую сведения о сроках ее приостановления.

Органы, уполномоченные на ведение лицензионной деятельности, ежеквартально представляют в Межведомственную комиссию сведения о выданных и аннулированных лицензиях.

Контроль за соблюдением лицензионных условий лицензиатами, выполняющими работы, связанные с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны, осуществляют органы, уполномоченные на ведение лицензионной деятельности.

Решения и действия органов, уполномоченных на ведение лицензионной деятельности, могут быть обжалованы в установленном порядке.

Рис. 2.16. Блок-схема последовательности действий при исполнении государственной функции

За предоставление лицензирующим органом лицензии, переоформление документа, подтверждающего наличие лицензии, выдачу дубликата документа, подтверждающего наличие лицензии, и продление срока действия лицензии уплачивается государственная пошлина в размерах и порядке, которые установлены законодательством Российской Федерации о налогах и сборах (рис. 2.16).

2.14. Специальные экспертизы предприятий

Федеральная служба безопасности Российской Федерации, Федеральная служба по техническому и экспортному контролю, Служба внешней разведки Российской Федерации, Министерство обороны Российской Федерации, другие министерства и ведомства Российской Федерации, руководители которых наделены полномочиями по отнесению к государственной тайне сведений в отношении подведомственных им предприятий, на основании приведенного Положения разработали свои ведомственные инструкции о порядке проведения специальных экспертиз по допуску предприятий, учреждений и организаций к проведению работ, связанных с использованием сведений, составляющих государственную тайну. В частности, такая Инструкция была утверждена Приказом ФСБ РФ 23 августа 1995 г. № 28.

Данная Инструкция определяет порядок организации и проведения специальных экспертиз предприятий, учреждений и организаций (далее – предприятия) на право осуществления ими работ, связанных с использованием сведений, составляющих государственную тайну (далее – специальная экспертиза), на территории Российской Федерации.

Специальные экспертизы предприятий выполняются по следующим направлениям:

– режим секретности;

– противодействие иностранной технической разведке;

– защита информации от утечки по техническим каналам.

Специальные экспертизы организуются и проводятся:

– Федеральной службой безопасности Российской Федерации и территориальными органами безопасности, ФСТЭК России, и их органами на местах, другими министерствами и ведомствами Российской Федерации, руководители которых наделены полномочиями по отнесению к государственной тайне сведений в отношении подведомственных им предприятий;

– отраслевыми аттестационными центрами министерств и ведомств, руководители которых наделены полномочиями по отнесению сведений к государственной тайне, для проведения специальных экспертиз на подведомственных им предприятиях (отраслевые аттестационные центры при необходимости могут проводить специальные экспертизы вневедомственных предприятий);

– региональными аттестационными центрами Федеральной службы безопасности Российской Федерации и территориальными органами безопасности, ФСТЭК России, и их органами на местах, а также администрациями субъектов Российской Федерации, для проведения экспертиз на вневедомственных предприятиях.

Проведение специальных экспертиз осуществляется экспертными комиссиями.

Экспертные комиссии формируются при Федеральной службе безопасности Российской Федерации и территориальных органах безопасности, ФСТЭК России, и их органах на местах и аттестационных центрах.

В состав экспертных комиссий могут включаться представители Федеральной службы безопасности Российской Федерации и территориальных органов безопасности, ФСТЭК России, и их органов на местах, других министерств, ведомств и предприятий из числа специалистов, компетентных в соответствующих областях защиты государственной тайны (режим секретности, противодействие иностранной технической разведке, защита информации от утечки по техническим каналам) и имеющих необходимую форму допуска к работе со сведениями, составляющими государственную тайну.

Составы экспертных комиссий утверждаются Федеральной службой безопасности Российской Федерации или территориальными органами безопасности по согласованию с подразделениями, осуществляющими лицензионную деятельность, ФСТЭК России, или с их органами на местах.

Для проведения специальных экспертиз предприятия обращаются в Федеральную службу безопасности Российской Федерации или в территориальные органы безопасности.

Обращение предприятия для проведения специальной экспертизы оформляется в произвольной форме и подписывается руководителем (или заместителем руководителя) предприятия.

В обращении указывается:

– наименование и организационно-правовая форма предприятия, его юридический адрес, номер расчетного счета в банке;

– ведомственная принадлежность предприятия и контактный телефон.

Федеральная служба безопасности Российской Федерации или территориальный орган безопасности на основании обращения предприятия о проведении специальной экспертизы с участием ФСТЭК России или их органов на местах дает соответствующее поручение аттестационному центру (экспертной комиссии в случае проведения специальной экспертизы Федеральной службой безопасности Российской Федерации или территориальным органом безопасности) и уведомляет об этом предприятие.

Сроки работы экспертной комиссии доводятся до руководства предприятия не позднее чем за пять дней до начала ее работы.

Результаты работы экспертной комиссии оформляются актом, утверждаемым ее председателем.

В акте специальной экспертизы дается заключение о готовности (неготовности) предприятия осуществлять работы, связанные с использованием сведений, составляющих государственную тайну.

Акт специальной экспертизы прилагается к заявлению о выдаче лицензии, которое направляется предприятием в Федеральную службу безопасности Российской Федерации, территориальный орган безопасности.

Специальная экспертиза проводится по договору между предприятием и органом лицензирования или аттестационным центром, ее проводящим.

Основанием для заключения предприятием договора на проведение специальной экспертизы с Федеральной службой безопасности Российской Федерации, территориальным органом безопасности или аттестационным центром является уведомление предприятия Федеральной службой безопасности Российской Федерации или территориальным органом безопасности о проведении специальной экспертизы.

Оплата работы членов экспертной комиссии осуществляется в порядке, установленном органом лицензирования или аттестационным центром, с которым предприятием заключался договор на проведение специальной экспертизы.

Специальные экспертизы проводятся путем оценки готовности выполнения предприятиями следующих условий:

– выполнения требований законодательных и иных нормативных актов Российской Федерации по обеспечению защиты сведений, составляющих государственную тайну, в процессе выполнения работ, связанных с использованием указанных сведений;

– достаточности количества и уровня квалификации специально подготовленных сотрудников по защите государственной тайны и защите информации;

– наличия сертифицированных средств защиты информации.

Оценка готовности выполнения предприятиями требований законодательных и иных нормативных актов Российской Федерации по обеспечению защиты сведений, составляющих государственную тайну, в процессе выполнения работ, связанных с использованием указанных сведений, предусматривает проверку:

– наличия законодательных и нормативных актов Российской Федерации по обеспечению защиты сведений, составляющих государственную тайну, а также нормативно-методических документов по режиму секретности, противодействию иностранной технической разведке и защите информации от утечки по техническим каналам, утверждаемых Федеральной службой безопасности

Российской Федерации, ФСТЭК России с учетом специфики деятельности предприятий;

– наличия и качества разработки предприятиями документов, регламентирующих организацию и порядок проведения на предприятиях работ по защите сведений, составляющих государственную тайну;

– наличия аттестованных объектов информатики (под объектами информатики понимаются автоматизированные системы различного уровня и назначения, системы связи, отображения и размножения вместе с помещениями, в которых они установлены, предназначенные для обработки и передачи секретной информации, а также помещения, предназначенные для ведения секретных переговоров), кроме органов шифровальной службы;

– наличия в структуре предприятия соответствующих подразделений по защите государственной тайны.

Оценка достаточности количества и уровня квалификации специально подготовленных сотрудников (кроме сотрудников шифровальной службы) по защите государственной тайны и защите информации предусматривает проверку их готовности выполнять следующие виды работ:

– определение охраняемых сведений, демаскирующих признаков предприятия и его производственной деятельности;

– проведение анализа возможностей технической разведки в отношении предприятий по добыванию сведений, составляющих государственную тайну;

– выявление каналов утечки сведений, составляющих государственную тайну;

– разработка мероприятий по защите сведений о предприятии и выпускаемой продукции, составляющих государственную тайну, и оценка их достаточности;

– аттестация рабочих мест по всему технологическому циклу разработки, изготовления и испытания продукции, подлежащей защите;

– контроль выполнения применяемых мер защиты сведений, составляющих государственную тайну.

Кроме того, в ходе проверки при необходимости оценивается достаточность проводимых предприятиями организационных и технических мероприятий по защите сведений, составляющих государственную тайну, в соответствии с требованиями законодательных и нормативных актов Российской Федерации и нормативно-методических документов.

Оценка наличия сертифицированных средств защиты информации заключается в проверке прохождения предполагаемыми к использованию средствами защиты информации установленных процедур сертификации на выполнение требований по защите сведений соответствующей степени секретности.

Отраслевые аттестационные центры создаются совместным решением министерств и ведомств, руководители которых наделены полномочиями по отнесению сведений к государственной тайне, Федеральной службы безопасности Российской Федерации и ФСТЭК России.

Региональные аттестационные центры создаются совместным решением Федеральной службы безопасности Российской Федерации и ФСТЭК России. Это решение принимается также совместно с администрацией субъекта Российской Федерации, если она обратилась в указанные органы с предложением о создании такого центра.

Отраслевые и региональные аттестационные центры получают лицензии в установленном порядке.

Специальные экспертизы аттестационных центров проводятся экспертными комиссиями, сформированными из специалистов Федеральной службы безопасности Российской Федерации или территориальных органов безопасности, ФСТЭК России или их органов на местах.

Состав экспертной комиссии формируется Федеральной службой безопасности Российской Федерации или территориальными органами безопасности по согласованию с ФСТЭК России или их органами на местах.

Контрольные вопросы

1. Какие органы государственной тайны обеспечивают защиту государственной тайны?

2. Каковы основания для засекречивания сведений?

3. Какие принципы отнесения сведений к государственной тайне и засекречивания этих сведений?

4. Какие сведения не подлежат отнесению к государственной тайне и засекречиванию?

5. Каковы правила отнесения сведений, составляющих государственную тайну, к различным степеням секретности?

6. Как осуществляется передача сведений, составляющих государственную тайну?

7. Как осуществляется передача сведений, составляющих государственную тайну, другим государствам?

8. Чем отличается допуск от доступа к сведениям, составляющим государственную тайну?

9. Что предусматривает допуск граждан к государственной тайне?

10. Какие основания могут являться для отказа гражданину в допуске к государственной тайне?

11. Кто принимает решение о допуске к государственной тайне граждан?

12. В каких случаях допуск гражданина к государственной тайне может быть прекращен?

13. Какие основные вопросы содержит Анкета гражданина?

14. Кем осуществляются Проверочные мероприятия, связанные с допуском граждан к сведениям, составляющим государственную тайну?

15. Что является Целью проведения проверочных мероприятий?

16. Как принимается решение о допуске работника, принятого на работу по совместительству?

17. В каких случаях допуск к государственной тайне не переоформляется?

18. Каким образом осуществляется доступ граждан к сведениям, составляющим государственную тайну, в организациях, в которые они командируются?

19. Каким образом обеспечиваются социальные гарантии гражданам, допущенным к государственной тайне на постоянной основе, и сотрудникам структурных подразделений по защите государственной тайны? Какие нарушения правил обращения с государственной тайной влекут за собой административно-правовую ответственность?

20. Кто несет административно-правовую ответственность за эти нарушения?

21. Какими статьями Кодекса РФ об административных правонарушениях предусмотрена эта административно-правовая ответственность?

22. Какие взыскания административно-правового характера предусмотрены за указанные нарушения?

23. Какие государственные органы и их должностные лица уполномочены назначать административно-правовые взыскания за нарушения правил обращения с государственной тайной?

24. Какие посягательства на государственную тайну признаются преступлениями по Уголовному кодексу РФ?

25. Какие действия образуют шпионаж первого вида?

26. Каковы условия освобождения от уголовной ответственности лиц, совершивших государственную измену или шпионаж?

27. Чем разглашение тайны отличается от государственной измены?

28. Кто несет уголовную ответственность за разглашение государственной тайны?

29. Какой порядок допуска предприятий, учреждений и организаций к проведению работ, связанных с использованием сведений, составляющих государственную тайну?

30. Какой порядок подготовки сотрудников для работы по защите информации, составляющей государственную тайну?

31. Какой порядок сертификации средств защиты информации?

32. Каким образом осуществляется финансирование мероприятий по защите государственной тайны?

33. Как осуществляется федеральный государственный контроль за обеспечением защиты государственной тайны?

34. Какие органы уполномочены на ведение лицензионной деятельности?

35. Что возлагается на орган, уполномоченный на ведение лицензионной деятельности?

36. В каких случаях приостанавливается действие лицензии или ее аннулируют?

37. Какой порядок проведения специальных экспертиз предприятий?

Глава 3

ЗАЩИТА ГОСУДАРСТВЕННОЙ ТАЙНЫ ПРИ УГОЛОВНО-ПРОЦЕССУАЛЬНОЙ И ОПЕРАТИВНО-РАЗЫСКНОЙ ДЕЯТЕЛЬНОСТИ

Никогда не доверяйте ваших тайн бумаге – это все равно,
что бросить камень в воздух: если знаешь, кто бросил его,
то не знаешь, куда он упадет.

Педро де Кальдерон

3.1. Защита государственной тайны в уголовном процессе

Вопросы защиты государственной тайны приобрели особую значимость в последние годы – в период глубоких социально-экономических преобразований в Российской Федерации, когда, с одной стороны, появляются новые угрозы безопасности государства, а с другой стороны, сложившиеся режимы защиты государственной тайны перестают работать должным образом.

В этих условиях все большее значение имеют проводимые исследования норм, регулирующих вопросы, связанные с определением и защитой государственной тайны, правовым институтом тайны в целом. Актуальность таких исследований обусловлена тем, что правовой институт тайны, как совершенно справедливо отмечается в литературе, является одним из важнейших институтов, определяющих соотношение интересов личности, общества и государства, частного и публичного начала права, основания и пределы вмешательства государства

в негосударственную сферу, степень информационной защищенности в Российской Федерации.

Исследования государственной тайны и других видов тайн проводятся как с позиции общей теории права, так и отраслей права, в том числе уголовно-процессуального, в рамках которого выделяется «тайноведческий уголовный процесс».

Исходя из характера уголовно-процессуальной деятельности как деятельности уполномоченных государственных органов и их должностных лиц, а также из интересов государства по обеспечению сохранности государственной тайны, одним из приоритетных направлений таких исследований являются вопросы защиты государственной тайны в уголовном судопроизводстве, т. е. досудебном и судебном производстве по уголовным делам.

Защиту государственной тайны при осуществлении уголовно-процессуальной деятельности можно рассматривать в двух аспектах:

– специальный порядок получения при производстве уголовно-процессуальных действий сведений, составляющих государственную тайну;

– специальный порядок допуска к материалам уголовных дел, содержащих государственную тайну.

Специальный порядок получения составляющих государственную тайну сведений распространяется как на стадию предварительного расследования и последующие стадии уголовного судопроизводства, когда уголовное дело уже возбуждено, так и на стадию возбуждения уголовного дела, когда проводится предварительная (доследственная) проверка, предусмотренная ст. 144 Уголовно-процессуального кодекса Российской Федерации (далее по тексту — УПК России), целью которой является установление оснований к возбуждению уголовного дела, либо производится прокурорская проверка при осуществлении прокурорского надзора.

Необходимо иметь в виду, что дознаватель, орган дознания и следователь, проверяя сообщение о преступлении, могут истребовать из предприятий, учреждений и организаций необходимые материалы и получать объяснения, в том числе истребовать носители

сведений, составляющих государственную тайну, а также получать объяснения от лиц, обладающих сведениями, составляющими государственную тайну.

Возможность осуществления указанных действий до возбуждения уголовного дела закреплена в ряде нормативных правовых актов.

Например, ст. 11 Закона Российской Федерации «О полиции» определено, что полиции для выполнения возложенных на нее обязанностей предоставляется право вызывать граждан и должностных лиц по находящимся в производстве материалам, получать от граждан и должностных лиц необходимые объяснения, сведения, справки, документы и копии с них.

Статья 22 Федерального закона «О прокуратуре Российской Федерации» предусмотрено, что прокурор при осуществлении возложенных на него функций вправе по предъявлении служебного удостоверения иметь доступ к документам и материалам, включая содержащие сведения, составляющие государственную тайну, федеральных министерств, служб и иных федеральных органов исполнительной власти, представительных (законодательных) и исполнительных органов государственной власти субъектов Российской Федерации, органов местного самоуправления, военного управления, контроля, а также коммерческих и некоммерческих организаций. Он вправе требовать от руководителей и должностных лиц этих органов и организаций предоставления необходимых документов, материалов, статистических и иных сведений, вызывать должностных лиц и граждан для объяснений по поводу нарушений законов.

Согласно ст. 6 Федерального закона «О прокуратуре Российской Федерации», требования прокурора, вытекающие из указанных полномочий, подлежат безусловному исполнению в установленный срок, а неисполнение требований прокурора и следователя, вытекающих из их полномочий, а также уклонение от явки по их вызову влекут за собой установленную законом ответственность.

Согласно ст. 13 Федерального закона «О Федеральной службе безопасности», органы Федеральной службы безопасности имеют

право получать от государственных органов, предприятий, учреждений и организаций независимо от форм собственности информацию, необходимую для выполнения возложенных на органы федеральной службы безопасности обязанностей, за исключением случаев, когда федеральными законами установлен запрет на передачу такой информации органам федеральной службы безопасности.

За невыполнение этих требований предусмотрена ответственность. Так, например, ст. 17.7 Кодекса Российской Федерации об административных правонарушениях предусмотрено, что умышленное невыполнение требований прокурора, вытекающих из его полномочий, установленных федеральным законом, а равно законных требований следователя или дознавателя, влечет наложение административного штрафа на граждан и должностных лиц. Если лицо, от которого получено объяснение, считает, что действия по истребованию и получению объяснения привели к нарушению его прав, свобод и законных интересов, то оно вправе обжаловать такие действия лиц, осуществляющих доследственную проверку, в вышестоящих органах или у должностных лиц, прокурора либо в суде.

Как предусмотрено п. 7 ч. 2 ст. 29 и ч. 3 с. 183 УПК России, выемка предметов и документов, содержащих государственную тайну (эта формулировка использована в УПК, хотя следует говорить о предметах и документах как носителях сведений, составляющих государственную тайну), производится на основании судебного решения, принимаемого в порядке ст. 165 УПК России, а именно – следователь с согласия руководителя следственного органа возбуждает перед судом ходатайство о производстве указанного следственного действия, о чем выносится постановление.

При этом сотрудники правоохранительных органов, получившие информацию, содержащую государственную тайну, обязаны создать условия, обеспечивающие ее защиту. Они несут установленную законом персональную ответственность за ее сохранность, в том числе за несоблюдение установленных ограничений

по ознакомлению третьих лиц со сведениями, составляющими государственную тайну.

В связи с данным обстоятельством необходимо четкое нормативное определение оснований и условий доступа либо отказа в доступе к сведениям, составляющим государственную тайну, лиц, вовлеченных в орбиту уголовно-процессуальной деятельности.

Контроль и надзор за обеспечением защиты государственной тайны при осуществлении уголовно-процессуальной и оперативно-разыскной деятельности осуществляется с учетом положений ст. 25, 30–32 Закона Российской Федерации «О государственной тайне».

При этом межведомственный контроль за обеспечением защиты государственной тайны в федеральных органах исполнительной власти, наделенных правом осуществления уголовно-процессуальной деятельности, осуществляют в пределах их полномочий 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, на которые эта функция возложена законодательством Российской Федерации.

Соответствующие органы государственной власти, наделенные полномочиями по распоряжению сведениями, составляющими государственную тайну, обязаны контролировать эффективность защиты этих сведений во всех подчиненных и подведомственных им органах.

Контроль за обеспечением защиты государственной тайны в судебных органах и органах прокуратуры организуется руководителями этих органов.

Надзор за соблюдением законодательства при обеспечении защиты государственной тайны и законностью принимаемых при этом решений осуществляют Генеральный прокурор Российской Федерации и подчиненные ему прокуроры.

Доступ лиц, осуществляющих прокурорский надзор, к сведениям, составляющим государственную тайну, осуществляется в соответствии со ст. 25 Закона Российской Федерации «О государственной тайне».

В Модельном уголовно-процессуальном кодексе для государств – участников СНГ, принятом на седьмом пленарном заседании Межпарламентской Ассамблеи государств – участников Содружества Независимых Государств 17 февраля 1996 г. Указанный рекомендательный законодательный акт содержит специальную статью, названную «Охрана государственной тайны»:

«1. В ходе уголовного судопроизводства принимаются предусмотренные настоящим Кодексом и другими законами меры по охране получаемых сведений, составляющих государственную тайну.

2. Лица, которым орган, ведущий уголовный процесс, предлагает сообщить или представить составляющие государственную тайну сведения, имеют право убедиться в том, что эти сведения собираются по возбужденному уголовному делу, и в противном случае — отказать в сообщении или предоставлении сведений. Лица, которым орган уголовного преследования предлагает в соответствии с положениями настоящего Кодекса сообщить или предоставить составляющие государственную тайну сведения, не могут отказаться от выполнения этого требования со ссылкой на необходимость соблюдения государственной тайны, но вправе предварительно получить от следователя, дознавателя подлежащее внесению в протокол допроса или другого соответствующего действия разъяснение, подтверждающее необходимость получения указанных сведений органом уголовного преследования.

3. Государственный служащий, давший показания в отношении составляющих государственную тайну сведений, ему вверенных, письменно сообщает об этом руководителю соответствующего государственного органа, если это не будет ему прямо запрещено органом, ведущим уголовный процесс.

4. Производство по уголовным делам, связанным с составляющими государственную тайну сведениями, поручается судьям,

а также следователям, дознавателям, давшим подписку о неразглашении таких сведений. Обязательство хранить составляющие государственную тайну сведения включается в присягу, которую принимает присяжный заседатель перед началом судебного следствия по уголовному делу, содержащему такие сведения. Присяжные заседатели по указанным делам дают подписку о неразглашении составляющих государственную тайну сведений; при отказе от дачи такой подписки присяжный заседатель освобождается от участия в уголовном судопроизводстве по соответствующему делу.

5. Защитники и другие представители, а также иные лица, которым для целей производства по уголовному делу будут представлены для ознакомления или иным способом сообщены составляющие государственную тайну сведения, должны предварительно дать подписку о неразглашении такта сведений. В случае отказа дать такую подписку защитник и другой представитель, кроме законного представителя, лишаются права участвовать в уголовном судопроизводстве, а прочие лица не получают составляющих государственную тайну сведений. Данное участником процесса обязательство о неразглашении не препятствует ему требовать исследования составляющих государственную тайну сведений в закрытом заседании суда».

3.2. Защита государственной тайны и оперативно-разыскная деятельность

Вопросы защиты государственной тайны применительно к оперативно-разыскной деятельности можно рассматривать в нескольких аспектах:

– согласно ст. 2 Закона об ОРД как задачи оперативно-разыскной деятельности, а именно: выявление, предупреждение, пресечение и раскрытие преступлений, предметом которых являются сведения, составляющие государственную тайну, а также выявление и установление лиц, их подготавливающих, совершающих или совершивших, и добывание информации о событиях или действиях, касающихся отношений защиты государственной тайны

и создающих угрозу государственной, военной, экономической или экологической безопасности Российской Федерации.

– как предусмотренную ст. 7 Закона об ОРД оперативно-разыскную деятельность уполномоченных органов по сбору данных, необходимых для принятия решений о допуске к сведениям, составляющим государственную тайну.

– как специальный порядок защиты составляющих государственную тайну сведений, относящихся к оперативно-разыскной деятельности.

В соответствии с Федеральным законом от 20.02.1995 № 24-ФЗ «Об информации, информатизации и защите информации» и заменившим его Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» режим защиты информации в отношении сведений, отнесенных к государственной тайне, устанавливается уполномоченными органами на основании Закона Российской Федерации «О государственной тайне».

В то же время отдельные положения, касающиеся защиты сведений, составляющих государственную тайну, содержатся и в ряде других законов.

Так, согласно ст. 12 Закона об ОРД сведения об используемых или использованных при проведении негласных оперативно-разыскных мероприятий силах, средствах, источниках, методах, планах и результатах оперативно-разыскной деятельности, о лицах, внедренных в организованные преступные группы, о штатных негласных сотрудниках органов, осуществляющих оперативно-разыскную деятельность, и о лицах, оказывающих им содействие на конфиденциальной основе, а также об организации и о тактике проведения оперативно-разыскных мероприятий составляют государственную тайну и подлежат рассекречиванию только на основании постановления руководителя органа, осуществляющего оперативно-разыскную деятельность.

Предание гласности сведений о лицах, внедренных в организованные преступные группы, о штатных негласных сотрудниках органов, осуществляющих оперативно-разыскную деятельность, а также о лицах, оказывающих или оказывавших им содействие

на конфиденциальной основе, допускается лишь с их согласия в письменной форме и в случаях, предусмотренных федеральными законами.

Письменное согласие необходимо получать и при решении вопроса о возбуждении уголовных дел о разглашении составляющих государственную тайну сведений об этих лицах.

Если согласие получено, для защиты лиц, занимающих процессуальное положение, предусмотренное ч. 9 ст. 166 УПК России, следователем с согласия руководителя следственного органа может выноситься постановление о сохранении в тайне данных о личности этих лиц и в дальнейшем в протоколах следственных действий указывается псевдоним такого участника следственного действия.

Специальный порядок защиты составляющих государственную тайну сведений, относящихся к оперативно-разыскной деятельности, распространяется и на представление таких сведений другим органам для их использования.

В соответствии со ст. 11 Закона об ОРД результаты оперативно-разыскной деятельности могут быть использованы для подготовки и осуществления следственных и судебных действий, проведения оперативно-разыскных мероприятий по выявлению, предупреждению, пресечению и раскрытию преступлений, выявлению и установлению лиц, их подготавливающих, совершающих или совершивших, а также для розыска лиц, скрывшихся от органов дознания, следствия и суда, уклоняющихся от исполнения наказания и без вести пропавших.

Кроме того, результаты оперативно-разыскной деятельности могут служить поводом и основанием для возбуждения уголовного дела, представляться в орган дознания, следователю или в суд, в производстве которого находится уголовное дело, а также использоваться в доказывании по уголовным делам в соответствии с положениями уголовно-процессуального законодательства Российской Федерации, регламентирующими собирание, проверку и оценку доказательств.

Представление результатов оперативно-разыскной деятельности органу дознания, следователю или в суд осуществляется на

основании постановления руководителя органа, осуществляющего оперативно-разыскную деятельность, в порядке, предусмотренном ведомственными нормативными актами.

Как уже отмечалось, дознавателю, органу дознания, следователю или в суд могут представляться результаты оперативно-разыскной деятельности, содержащие сведения, относящиеся к государственной тайне. В этом случае они представляются в соответствии с требованиями ст. 16 Закона Российской Федерации «О государственной тайне», регулирующей вопросы взаимной передачи сведений, составляющих государственную тайну, органами государственной власти, предприятиями, учреждениями и организациями.

В то же время, если использование результатов оперативно-разыскной деятельности в уголовном процессе создает реальную возможность расшифровки (разглашения) сведений об используемых или использованных при проведении оперативно-разыскных мероприятий негласных силах, средствах, источниках, методах и планах, о лицах, внедренных в организованные преступные группы, о штатных негласных сотрудниках органов, осуществляющих оперативно-разыскную деятельность, о лицах, оказывающих им содействие на конфиденциальной основе, а также об организации и тактике проведения оперативно-разыскных мероприятий, отнесенных законом к государственной тайне, результаты оперативно-разыскной деятельности могут не представляться.

Решение о непредоставлении результатов оперативно-разыскной деятельности по этим мотивам оформляется постановлением руководителя органа, осуществляющего оперативно-разыскную деятельность, и приобщается к материалам дела оперативного учета или соответствующего номенклатурного дела. О принятом решении уведомляется инициатор запроса о предоставлении результатов оперативно-разыскной деятельности.

Специальный порядок защиты составляющих государственную тайну сведений, относящихся к оперативно-разыскной деятельности, включает и оперативно-разыскную деятельность уполномоченных субъектов по сбору данных, необходимых для

принятия решений о допуске к сведениям, составляющим государственную тайну.

Оперативно-разыскная деятельность уполномоченных органов по сбору данных, необходимых для принятия решений о допуске к сведениям, составляющим государственную тайну.

Законом Российской Федерации «О государственной тайне» определено, что допуск к государственной тайне есть процедура оформления права граждан на доступ к сведениям, составляющим государственную тайну.

Порядок допуска к государственной тайне определен Инструкцией о порядке допуска должностных лиц и граждан Российской Федерации к государственной тайне, утвержденной постановлением Правительства Российской Федерации от 06.02.2010 № 63, регламентирующей, в частности, вопросы, связанные с проведением проверочных мероприятий в отношении лиц, получающих соответствующий допуск. Специальный порядок допуска отдельных категорий лиц к такого рода сведениям определен Положением о порядке допуска лиц, имеющих двойное гражданство, лиц без гражданства, а также лиц из числа иностранных граждан, эмигрантов и реэмигрантов к государственной тайне, утвержденным Постановлением Правительства Российской Федерации от 22.08.1998 № 1003.

Контрольные вопросы

1. В каких аспектах можно рассматривать Вопросы защиты государственной тайны применительно к оперативно-разыскной деятельности?
2. В соответствии с какой статьей результаты оперативно-разыскной деятельности могут быть использованы для подготовки и осуществления следственных и судебных действий?
3. Представление результатов оперативно-разыскной деятельности органу дознания, следователю или в суд осуществляется на основании чего?
4. Решение о непредоставлении результатов оперативно-разыскной деятельности по этим мотивам оформляется органом?
5. Что включает Специальный порядок защиты составляющих государственную тайну сведений, относящихся к оперативно-разыскной деятельности?

Глава 4

ЗАЩИТА ИНФОРМАЦИИ, СОСТАВЛЯЮЩЕЙ ГОСУДАРСТВЕННУЮ ТАЙНУ, ОТ ИНОСТРАННЫХ ТЕХНИЧЕСКИХ РАЗВЕДОК И ОТ ЕЕ УТЕЧКИ ПО ТЕХНИЧЕСКИМ КАНАЛАМ

4.1. Государственная система защиты информации

Постановлением Совета Министров – Правительства Российской Федерации от 15.09.1993 № 912-51 утверждено Положение о государственной системе защиты информации в Российской Федерации от иностранных технических разведок и от ее утечки по техническим каналам (рис. 4.1, 4.2, 4.3).

Положение определяет структуру государственной системы защиты информации в Российской Федерации, ее задачи и функции, основы организации защиты сведений, отнесенных в установленном порядке к государственной или служебной тайне, от иностранных технических разведок и от ее утечки по техническим каналам (далее именуется – защита информации).

Главными направлениями работ по защите информации являются:

– обеспечение эффективного управления системой защиты информации;

– определение сведений, охраняемых от технических средств разведки, и демаскирующих признаков, раскрывающих эти сведения;

– анализ и оценка реальной опасности перехвата информации техническими средствами разведки, несанкционированного

Рис. 4.1. Основные задачи государственной системы противодействия иностранным техническим разведкам (ПД ИТР) и технической защиты информации (ТЗИ)

Рис. 4.2. Структура государственной системы противодействия иностранным техническим разведкам и технической защиты информации

Рис. 4.3. Структура организации противодействия иностранным техническим разведкам и технической защиты информации

доступа, разрушения (уничтожения) или искажения информации путем преднамеренных программно-технических воздействий в процессе ее обработки, передачи и хранения в технических средствах, выявление возможных технических каналов утечки сведений, подлежащих защите;

– разработка организационно-технических мероприятий по защите информации и их реализация;

– организация и проведение контроля состояния защиты информации.

Основными организационно-техническими мероприятиями по защите информации являются:

– лицензирование деятельности предприятий в области защиты информации;

– аттестация объектов по выполнению требований обеспечения защиты информации при проведении работ со сведениями соответствующей степени секретности;

– сертификация средств защиты информации и контроля за ее эффективностью, систем и средств информатизации и связи в части защищенности информации от утечки по техническим каналам;

– категорирование вооружения и военной техники, предприятий (объектов) по степени важности защиты информации в оборонной, экономической, политической, научно-технической и других сферах деятельности;

– обеспечение условий защиты информации при подготовке и реализации международных договоров и соглашений;

– оповещение о пролетах космических и воздушных летательных аппаратов, кораблях и судах, ведущих разведку объектов (перехват информации, подлежащей защите), расположенных на территории Российской Федерации;

– введение территориальных, частотных, энергетических, пространственных и временных ограничений в режимах использования технических средств, подлежащих защите;

– создание и применение информационных и автоматизированных систем управления в защищенном исполнении;

– разработка и внедрение технических решений и элементов защиты информации при создании и эксплуатации вооружения и военной техники, при проектировании, строительстве (реконструкции) и эксплуатации объектов, систем и средств информатизации и связи;

– разработка средств защиты информации и контроля за ее эффективностью (специального и общего применения) и их использование;

– применение специальных методов, технических мер и средств защиты, исключающих перехват информации, передаваемой по каналам связи.

Основные задачи государственной системы защиты информации:

– проведение единой технической политики, организация и координация работ по защите информации в оборонной, экономической, политической, научно-технической и других сферах деятельности;

– исключение или существенное затруднение добывания информации техническими средствами разведки, а также предотвращение ее утечки по техническим каналам, несанкционированного доступа к ней, предупреждение преднамеренных программно-технических воздействий с целью разрушения (уничтожения) или искажения информации в процессе ее обработки, передачи и хранения;

– принятие в пределах компетенции правовых актов, регулирующих отношения в области защиты информации;

– анализ состояния и прогнозирование возможностей технических средств разведки и способов их применения, формирование системы информационного обмена сведениями по осведомленности иностранных разведок;

– организация сил, создание средств защиты информации и контроля за ее эффективностью;

– контроль состояния защиты информации в органах государственной власти и на предприятиях.

Организация работ по защите информации на предприятиях осуществляется их руководителями

В зависимости от объема работ по защите информации руководителем предприятия создается структурное подразделение по защите информации либо назначаются штатные специалисты по этим вопросам, которые подчиняются непосредственно руководителю предприятия или его заместителю.

Подразделения по защите информации (штатные специалисты) на предприятиях:

– осуществляют мероприятия по защите информации в ходе выполнения работ с использованием сведений, отнесенных к государственной или служебной тайне;

– определяют совместно с заказчиком работ основные направления комплексной защиты информации;

– участвуют в согласовании технических (тактико-технических) заданий на проведение таких работ;

– дают заключение о возможности проведения работ с информацией, содержащей сведения, отнесенные к государственной или служебной тайне.

Для проведения работ по защите информации могут привлекаться на договорной основе специализированные предприятия, имеющие лицензии на право проведения работ в области защиты информации.

В интересах обеспечения защиты информации в системах и средствах информатизации и связи защите подлежат:

– информационные ресурсы, содержащие сведения, отнесенные к государственной или служебной тайне, представленные в виде носителей на магнитной и оптической основе, информативных физических полей, информативных массивов и баз данных;

– средства и системы информатизации (средства вычислительной техники, информационно-вычислительные комплексы, сети и системы), программные средства (операционные системы, системы управления базами данных, другое общесистемное и прикладное программное обеспечение), автоматизированные системы управления, системы связи и передачи данных, технические средства приема, передачи и обработки информации (звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования

документов и другие технические средства обработки графической, смысловой и буквенно-цифровой информации), используемые для обработки информации, содержащей сведения, отнесенные к государственной или служебной тайне;

– технические средства и системы, не обрабатывающие информацию, но размещенные в помещениях, где обрабатывается (циркулирует) информация, содержащая сведения, отнесенные к государственной или служебной тайне, а также сами помещения, предназначенные для ведения секретных переговоров.

Целями защиты информации являются:

– предотвращение утечки информации по техническим каналам;

– предотвращение несанкционированного уничтожения, искажения, копирования, блокирования информации в системах информатизации;

– соблюдение правового режима использования массивов и программ обработки информации, а также обеспечение полноты, целостности и достоверности информации в системах обработки;

– сохранение возможности управления процессом обработки и пользования информацией.

Защита информации осуществляется путем:

– предотвращения перехвата техническими средствами информации, передаваемой по каналам связи;

– предотвращения утечки обрабатываемой информации за счет побочных электромагнитных излучений и наводок, создаваемых функционирующими техническими средствами, а также электроакустических преобразований;

– исключения несанкционированного доступа к обрабатываемой или хранящейся в технических средствах информации;

– предотвращения специальных программно-технических воздействий, вызывающих разрушение, уничтожение, искажение информации или сбои в работе средств информатизации;

– выявления возможно внедренных на объекты и в технические средства электронных устройств перехвата информации (закладных устройств);

– предотвращения перехвата техническими средствами речевой информации из помещений и объектов.

Предотвращение перехвата техническими средствами информации, передаваемой по каналам связи, достигается применением криптографических и иных методов и средств защиты, а также проведением организационно-технических и режимных мероприятий.

Предотвращение утечки обрабатываемой информации за счет побочных электромагнитных излучений и наводок, а также электроакустических преобразований достигается применением защищенных технических средств, аппаратных средств защиты, средств активного противодействия, экранированием зданий или отдельных помещений, установлением контролируемой зоны вокруг средств информатизации и другими организационными и техническими мерами.

Исключение несанкционированного доступа к обрабатываемой или хранящейся в технических средствах информации достигается применением специальных программно-технических средств защиты, использованием криптографических способов защиты, а также организационными и режимными мероприятиями.

Предотвращение специальных программно-технических воздействий, вызывающих разрушение, уничтожение, искажение информации или сбои в работе средств информатизации, *достигается* применением специальных программных и аппаратных средств защиты (антивирусных процессоров, антивирусных программ), организацией системы контроля безопасности программного обеспечения.

Выявление возможно внедренных на объекты и в технические средства электронных устройств перехвата информации (закладных устройств) достигается проведением специальных проверок по выявлению этих устройств.

Предотвращение перехвата техническими средствами речевой информации из помещений и объектов достигается применением специальных средств защиты, проектными решениями, обеспечивающими звукоизоляцию помещений, выявлением специальных устройств подслушивания и другими организационными и режимными мероприятиями.

Информация, содержащая сведения, отнесенные к государственной или служебной тайне, должна обрабатываться с использованием защищенных систем и средств информатизации и связи или с использованием технических и программных средств защиты, сертифицированных в установленном порядке.

Соответствие технического средства и его программного обеспечения требованиям защищенности подтверждается:

– сертификатом, выдаваемым предприятием, имеющим лицензию на этот вид деятельности;

– по результатам сертификационных испытаний;

– предписанием на эксплуатацию, оформляемым по результатам специальных исследований и специальных проверок технических средств и программного обеспечения.

Для оценки готовности систем и средств информатизации и связи к обработке (передаче) информации, содержащей сведения, отнесенные к государственной или служебной тайне, проводится аттестование указанных систем и средств в реальных условиях эксплуатации на предмет соответствия принимаемых методов, мер и средств защиты требуемому уровню безопасности информации.

Контроль состояния защиты информации осуществляется с целью своевременного выявления и предотвращения утечки информации по техническим каналам, несанкционированного доступа к ней, преднамеренных программно-технических воздействий на информацию и оценки защиты ее от иностранных технических разведок.

В зависимости от объема работ по защите информации руководителем предприятия (учреждения, организации) может быть создано структурное подразделение по защите информации либо назначаются штатные специалисты по этим вопросам;

Назначение и освобождение от должности руководителя подразделения по защите информации производится руководителем предприятия (учреждения, организации) по согласованию с вышестоящей организацией, курирующей вопросы защиты информации.

На структурное подразделение по защите информации либо штатного специалиста возлагаются следующие обязанности:

– выполняет работы по противодействию техническим разведкам;

– выполняет работы по выявлению каналов утечки информации и проведению мероприятий по использованию существующих методов и средств противодействия техническим разведкам;

– разрабатывает предложения по совершенствованию методов противодействия и оценки их эффективности;

– определяет цели и задачи работ, осуществляет проверку выполнения требований нормативных документов по противодействию техническим разведкам;

– возглавляет разработку проектов перспективных и текущих планов работ, составление отчетов по их выполнению;

– принимает участие в разработке технических заданий и проведении научных исследований, выполняемых в организации;

– готовит отзывы и заключения на проекты вновь строящихся зданий и сооружений;

– обеспечивает взаимодействие соисполнителей по научно-исследовательским и опытно-конструкторским работам в части обеспечения мер противодействия техническим разведкам;

– выполняет работы по технической защите информации в организациях;

– выявляет угрозы безопасности информации, определяет возможности технической разведки и проводит мероприятия технической защиты информации;

– проводит категорирование объектов информатизации;

– выявляет угрозы безопасности информации и технических каналов утечки информации, работах по проведению специальных проверок и специальных исследований объектов информатизации;

– формулирует цели и задачи работ по созданию безопасных информационных технологий, отвечающих требованиям технической защиты информации, определяет перспективы их развития для конкретных объектов защиты;

– участвует в организации и осуществлении мероприятий по предотвращению утечки информации ограниченного доступа должностными лицами организаций, выполняющих работы, связанные со сведениями, составляющими государственную тайну и (или) содержащими иную информацию ограниченного доступа;

– руководит работами по составлению актов, протоколов испытаний, предписаний на право эксплуатации и другой документации по обеспечению мероприятий противодействия техническим разведкам;

– участвует в разработке (доработке, модернизации) средств и систем, оценке технико-экономического уровня и эффективности предлагаемых и реализуемых решений в области противодействия техническим разведкам;

– определяет нарушения в применении способов и средств по противодействию техническим разведкам, разрабатывает меры по их устранению и предотвращению;

– участвует в экспертизе материалов, предназначенных для открытого опубликования;

– оценивает потребность и организует обеспечение (снабжение) техникой и оборудованием, а также материальными, финансовыми и другими ресурсами, обеспечивая их рациональное расходование.

Специалисты по защите информации должны знать:

– законы и иные нормативные правовые акты Российской Федерации, регулирующие отношения, связанные с защитой государственной тайны и иной информации ограниченного доступа;

– нормативные и методические документы по вопросам, связанным с обеспечением противодействия техническим разведкам;

– перспективы развития, специализацию, направления деятельности организации и ее подразделений;

– документы, определяющие основные направления экономического и социального развития организации; действующие системы сертификации, лицензирования, каналы утечки информации, способы их выявления, методы и средства контроля охраняемых сведений; показатели оценки эффективности мер по

противодействию техническим разведкам, методы их расчета и анализа, отыскания оптимальных решений по повышению эффективности противодействия техническим разведкам;

– достижения науки и техники в стране и за рубежом в области технических разведок и противодействия им; порядок заключения договоров на проведение специальных исследований, работ по защите основных и вспомогательных технических средств и систем; организацию взаимодействия подразделений при решении вопросов обеспечения по противодействию техническим разведкам и комплексного контроля;

– порядок финансирования, методы планирования и организации работ по противодействию техническим разведкам; порядок составления организационно-распорядительных документов, перспективных планов и программ проведения научных исследований, разработок, испытаний, внедрения новых технических средств по противодействию техническим разведкам; структуру, назначение, задачи, полномочия и техническую оснащенность отдела (лаборатории, сектора);

– основы эксплуатации специальной техники, организации ее обслуживания и ремонта; основы организации производства, труда и управления персоналом отдела (лаборатории, сектора);

– основы трудового законодательства; правила по охране труда и пожарной безопасности.

4.2. Обеспечение информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей

В соответствии с Указом Президента РФ от 17.03.2008 № 351 (ред. от 22.05.2015) «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена» устанавливается, что:

а) подключение информационных систем, информационно-телекоммуникационных сетей и средств вычислительной техники, применяемых для хранения, обработки или передачи информации,

содержащей сведения, составляющие государственную тайну, либо информации, обладателями которой являются государственные органы и которая содержит сведения, составляющие служебную тайну, к информационно-телекоммуникационным сетям, позволяющим осуществлять передачу информации через государственную границу Российской Федерации, в том числе к международной компьютерной сети Интернет (далее – информационно-телекоммуникационные сети международного информационного обмена), не допускается;

б) при необходимости подключения информационных систем, информационно-телекоммуникационных сетей и средств вычислительной техники, указанных в подпункте «*а*» настоящего пункта, к информационно-телекоммуникационным сетям международного информационного обмена такое подключение производится только с использованием специально предназначенных для этого средств защиты информации, в том числе шифровальных (криптографических) средств, прошедших в установленном законодательством Российской Федерации порядке сертификацию в Федеральной службе безопасности Российской Федерации и (или) получивших подтверждение соответствия в Федеральной службе по техническому и экспортному контролю. Выполнение данного требования является обязательным для операторов информационных систем, владельцев информационно-телекоммуникационных сетей и (или) средств вычислительной техники;

в) государственные органы в целях защиты общедоступной информации, размещаемой в информационно-телекоммуникационных сетях международного информационного обмена, используют только средства защиты информации, прошедшие в установленном законодательством Российской Федерации порядке сертификацию в Федеральной службе безопасности Российской Федерации и (или) получившие подтверждение соответствия в Федеральной службе по техническому и экспортному контролю;

г) размещение технических средств, подключаемых к информационно-телекоммуникационным сетям международного информационного обмена, в помещениях, предназначенных для

ведения переговоров, в ходе которых обсуждаются вопросы, содержащие сведения, составляющие государственную тайну, осуществляется только при наличии сертификата, разрешающего эксплуатацию таких технических средств в указанных помещениях. Финансирование расходов, связанных с размещением технических средств в указанных помещениях федеральных органов государственной власти, осуществляется в пределах бюджетных ассигнований, предусмотренных в федеральном бюджете на содержание этих органов.

4.3. Средства защиты информации

Средствами защиты информации являются технические, криптографические, программные и другие средства, предназначенные для защиты сведений, составляющих государственную тайну, средства, в которых они реализованы, а также средства контроля эффективности защиты информации.

Технические (аппаратные) средства – приборы, устройства, приспособления и другие технические решения, используемые в интересах защиты информации. Основная задача аппаратных средств — обеспечение стойкой защиты информации от разглашения, утечки и несанкционированного доступа через технические средства обеспечения производственной деятельности. Технические средства и методы защиты распространены достаточно широко. Однако из-за того, что они не обладают достаточной гибкостью, часто теряют свои защитные свойства при раскрытии их принципов действия и в дальнейшем не могут быть используемы. К техническим средствам защиты информации относятся самые различные по принципу действия, устройству и возможностям технические конструкции, обеспечивающие пресечение разглашения, защиту от утечки и противодействие несанкционированному доступу к источникам сведений, составляющих государственную тайну.

Криптографические средства — это специальные математические и алгоритмические средства защиты информации, передаваемой

по системам и сетям связи, хранимой и обрабатываемой на ЭВМ с использованием разнообразных методов шифрования. Криптографические методы занимают важное место и выступают надежным средством обеспечения защиты информации на длительные периоды. Криптография обеспечивает такую защиту секретной информации, что даже в случае ее перехвата посторонними лицами и обработки любыми способами с использованием самых быстродействующих ЭВМ и последних достижений науки и техники, она не должна быть дешифрована в течение нескольких десятков лет. Для такого преобразования информации используются различные шифровальные средства – такие, как средства шифрования документов, в том числе и портативного исполнения, средства шифрования речи (телефонных и радиопереговоров), телеграфных сообщений и передачи данных.

Программные средства – специальные программы, программные комплексы и системы защиты информации в информационных системах различного назначения и средствах обработки (сбора, накопления, хранения, обработки и передачи) данных. Программные средства и методы защиты надежны и период их гарантированного использования без перепрограммирования значительно больше, чем аппаратных.

Физические средства включают в себя различные средства и сооружения, препятствующие физическому проникновению (или доступу) злоумышленников на объекты защиты и к материальным носителям сведений, составляющих государственную тайну, и осуществляющие защиту персонала, материальных средств, финансов и информации от противоправных воздействий.

Средства контроля эффективности защиты информации представляют собой совокупность административных мер, осуществляемых в целях проверки и оценки фактического состояния режима секретности в ведомстве или на предприятии, своевременного выявления и предупреждения недостатков в его обеспечении. Само понятие контроля состоит в предупреждении несанкционированного доступа к защищенным данным. Контроль осуществляется, например, посредством составления списков

лиц, допущенных к материалам по той или иной программе, оформления дополнительных допусков. В ходе контроля эффективности защиты информации проверяется соответствие эффективности мероприятий по защите информации установленным требованиям, нормам эффективности защиты. Средствами контроля эффективности защиты информации могут являться проведение специальных экспертиз надежности защиты информации, проверки возможности несанкционированного доступа к секретной информации и другое.

4.4. Федеральная служба по техническому и экспортному контролю (ФСТЭК России)

В соответствии с Положением о Федеральной службе по техническому и экспортному контролю, введенным Указом Президента Российской Федерации от 16 августа 2004 г. № 1085, *Федеральная служба по техническому и экспортному контролю (ФСТЭК России) является федеральным органом исполнительной власти, осуществляющим реализацию государственной политики, организацию межведомственной координации и взаимодействия, специальные и контрольные функции в области государственной безопасности* по вопросам (рис. 4.4):

1) обеспечения безопасности информации в системах информационной и телекоммуникационной инфраструктуры, оказывающих существенное влияние на безопасность государства в информационной сфере (далее – безопасность информации в ключевых системах информационной инфраструктуры);

2) противодействия иностранным техническим разведкам на территории Российской Федерации (далее – противодействие техническим разведкам);

3) обеспечения защиты (некриптографическими методами) информации, содержащей сведения, составляющие государственную тайну, иной информации с ограниченным доступом, предотвращения ее утечки по техническим каналам, несанкционированного доступа к ней, специальных воздействий на информацию (носители информации) в целях ее добывания, уничтожения,

Рис. 4.4. Основные функции ФСТЭК России

искажения и блокирования доступа к ней на территории Российской Федерации (далее – техническая защита информации);

4) защиты информации при разработке, производстве, эксплуатации и утилизации неинформационных излучающих комплексов, систем и устройств;

5) осуществления экспортного контроля.

ФСТЭК России является федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, а также специально уполномоченным органом в области экспортного контроля.

ФСТЭК России является органом защиты государственной тайны, наделенным полномочиями по распоряжению сведениями, составляющими государственную тайну.

ФСТЭК России организует деятельность государственной системы противодействия техническим разведкам и технической защиты информации и руководит ею.

Руководство деятельностью ФСТЭК России осуществляет Президент Российской Федерации.

Основными задачами ФСТЭК России являются:

1) реализация в пределах своей компетенции государственной политики в области обеспечения безопасности информации в ключевых системах информационной инфраструктуры, противодействия техническим разведкам и технической защиты информации;

2) осуществление государственной научно-технической политики в области защиты информации при разработке, производстве, эксплуатации и утилизации неинформационных излучающих комплексов, систем и устройств;

3) организация деятельности государственной системы противодействия техническим разведкам и технической защиты информации на федеральном, межрегиональном, региональном, отраслевом и объектовом уровнях, а также руководство указанной государственной системой;

4) осуществление самостоятельного нормативно-правового регулирования вопросов:

– обеспечения безопасности информации в ключевых системах информационной инфраструктуры;

– противодействия техническим разведкам;

– технической защиты информации;

– размещения и использования иностранных технических средств наблюдения и контроля в ходе реализации международных договоров Российской Федерации, иных программ и проектов на территории Российской Федерации, на континентальном шельфе и в исключительной экономической зоне Российской Федерации;

– координации деятельности органов государственной власти по подготовке развернутых перечней сведений, подлежащих засекречиванию, а также методического руководства этой деятельностью;

– осуществления экспортного контроля;

5) обеспечение в пределах своей компетенции безопасности информации в ключевых системах информационной инфраструктуры, противодействия техническим разведкам и технической защиты информации в аппаратах федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации, в федеральных органах исполнительной власти, органах исполнительной власти субъектов Российской Федерации, органах местного самоуправления и организациях;

6) прогнозирование развития сил, средств и возможностей технических разведок, выявление угроз безопасности информации;

7) противодействие добыванию информации техническими средствами разведки, техническая защита информации;

8) осуществление координации деятельности федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации и организаций по государственному регулированию размещения и использования иностранных технических средств наблюдения и контроля в ходе реализации международных договоров Российской Федерации, иных программ и проектов на территории Российской Федерации, на континентальном шельфе и в исключительной экономической зоне Российской Федерации;

9) осуществление в пределах своей компетенции контроля деятельности по обеспечению безопасности информации в ключевых системах информационной инфраструктуры, по противодействию техническим разведкам и по технической защите информации в аппаратах федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации, в федеральных органах исполнительной власти, органах исполнительной власти субъектов Российской Федерации, органах местного самоуправления и организациях;

10) реализация государственной политики и организация межведомственного взаимодействия в области экспортного контроля;

11) осуществление контроля за соблюдением российскими участниками внешнеэкономической деятельности законодательных и иных нормативных правовых актов Российской Федерации в области экспортного контроля;

12) осуществление центральным аппаратом ФСТЭК России организационно-технического обеспечения деятельности Межведомственной комиссии по защите государственной тайны и Комиссии по экспортному контролю Российской Федерации.

Нормативные правовые акты и методические документы, изданные по вопросам деятельности ФСТЭК России, обязательны для исполнения аппаратами федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации, федеральными органами исполнительной власти, органами исполнительной власти субъектов Российской Федерации, органами местного самоуправления и организациями.

ФСТЭК России и ее территориальные органы входят в состав государственных органов обеспечения безопасности.

Деятельность ФСТЭК России обеспечивают Государственный научно-исследовательский испытательный институт проблем технической защиты информации ФСТЭК России (головная научная организация по проблемам защиты информации), а также другие подведомственные ФСТЭК России организации.

Контрольные вопросы

1. Какова структура государственной системы защиты информации в Российской Федерации, ее задачи и функции?

2. Какие главные направления работ по защите информации в Российской Федерации?

3. Какие основные организационно-технические мероприятиями по защите информации в Российской Федерации?

4. Какие основные задачи государственной системы защиты информации в Российской Федерации?

5. Что подлежит защите в системах и средствах информатизации и связи?

6. Какие цели защиты информации в Российской Федерации?

7. Как осуществляется защита информации в Российской Федерации?

8. Какие возлагаются обязанности на структурное подразделение либо штатного специалиста по защите информации?

9. Какие меры по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена установлены в Российской Федерации?

10. Что относится к средствам защиты информации? Их классификация и характеристики.

11. Какие функции выполняет Федеральная служба по техническому и экспортному контролю?

12. Каковы основные задачи Федеральной службы по техническому и экспортному контролю?

Глава 5

ЗАЩИТА ИНФОРМАЦИИ КОНФИДЕНЦИАЛЬНОГО ХАРАКТЕРА

Если секрет знают больше, чем двое, это уже не секрет.

Агата Кристи

Информационная безопасность является одним из важнейших аспектов интегральной безопасности, на каком бы уровне мы ни рассматривали последнюю — национальном, отраслевом, корпоративном или персональном. Информация может содержать элементы разрушительного, отравляющего, дезориентирующего, манипуляционного воздействия.

Информация – это власть. Еще древние жрецы понимали цену информационному противоборству: «Кто владеет информацией, тот владеет миром». Владение информацией во все времена давало преимущество той стороне, которая располагала более точной и обширной информацией, тем более если это касалось сведений о соперниках. Непреднамеренное или преднамеренное искажение информации, несанкционированный доступ к защищаемой информации может представлять значительную угрозу безопасности и способствовать резкому обострению политической, социальной, экономической, оборонной ситуации, наносить ущерб национальным интересам и даже привести к возникновению вооруженных конфликтов.

Как только человек понял, что всякое управление немыслимо без информации, он стал использовать в войнах информационное

оружие. Образование централизованных государств, формирование органов государственного управления, развитие международных связей привело к необходимости защиты информации в области военной, внешне- и внутриполитической деятельности государства. Вследствие этого информационная безопасность и является одной из важнейших составляющих государственной и национальной безопасности, роль и значение которой с каждым годом неуклонно возрастает.

Одним из наиболее важных факторов, влияющих на формирование общества являются информационно-коммуникационные технологии. Бурно развивающаяся информатизация привела к тому, что за последние годы проблема обеспечения информационной безопасности стала одной из основных глобальных проблем мирового сообщества. Помимо новых технических аспектов безопасности развитие средств обработки и передачи данных предопределило и рост преступности в этой сфере.

Объектами хакерских атак являются организации самых разных сфер — правительственные, военные, общественные, финансовые и т. п. Причем атаки происходят как из национального информационного пространства, так и из-за его внешних пределов.

В последние десятилетия сохраняется устойчивая тенденция к росту убытков, связанных с компьютерной преступностью. Наиболее часто фиксируемой формой нападения на компьютерные системы является несанкционированное изменение данных медицинских и финансовых учреждений.

Информационная безопасность является составной частью проблемы информационного обеспечения человека, государства и общества. Вследствие «проникновения» информатизации в повседневную жизнь граждан проблемы информационной безопасности прямо или косвенно стали касаться интересов практически каждого человека. Информационная сфера играет ключевую роль в реализации многих конституционных прав и свобод граждан, в обеспечении возможности самореализации личности, духовном обновлении, политической и социальной стабильности общества, обеспечении функционирования государства. Информационная сфера становится все более важным фактором развития

экономики промышленно развитых стран мира, мировой экономики в целом, развития мирового сообщества. При этом нормальная жизнедеятельность человеческого общества во все большей степени зависит от состояния информационной сферы, которая в связи с этим все активней используется для оказания «силового» давления на государственную политику тех или иных стран со стороны отдельных государств, международных и национальных террористических и преступных групп.

5.1. Система документов по защите сведений конфиденциального характера

В соответствии с Указом Президента РФ от 6.03.1997 № 188 «Об утверждении перечня сведений конфиденциального характера» в Российской Федерации определены сведения конфиденциального характера. К таковым относятся:

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

2. Сведения, составляющие *тайну следствия и судопроизводства*, сведения о лицах, в отношении которых в соответствии с федеральными законами от 20.04.1995 № 45-ФЗ «О государственной защите судей, должностных лиц правоохранительных и контролирующих органов» и от 20.08.2004 № 119-ФЗ «О государственной защите потерпевших, свидетелей и иных участников уголовного судопроизводства», другими нормативными правовыми актами Российской Федерации принято решение о применении мер государственной защиты, а также сведения о мерах государственной защиты указанных лиц, если законодательством Российской Федерации такие сведения не отнесены к сведениям, составляющим государственную тайну.

3. Служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с федеральными законами (**служебная тайна**).

4. Сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией Российской Федерации (ст. 23) и федеральными законами (**врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений и так далее**).

5. Сведения, связанные с коммерческой деятельностью, доступ к которым ограничен в соответствии с федеральными законами (**коммерческая тайна**).

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

7. Сведения, содержащиеся в личных делах осужденных, а также сведения о принудительном исполнении судебных актов, актов других органов и должностных лиц, кроме сведений, которые являются общедоступными в соответствии с Федеральным законом от 2.10.2007 № 229-ФЗ «Об исполнительном производстве» (пп. 3 ст. 6.1.).

Таким образом, сведения конфиденциального характера можно классифицировать следующим образом:

1. Персональные данные.
2. Тайна следствия и судопроизводства.
3. Служебная тайна.
4. Врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений и т. д.
5. Коммерческая тайна.

5.2. Принципы правового регулирования отношений в сфере информации, информационных технологий и защиты информации

Основополагающим законом в области регулирования отношений по осуществлению права на поиск, получение, передачу, производство и распространение информации; применения информационных технологий и обеспечения защиты информации является Закон Российской Федерации «Об информации,

информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ.

Этот закон определяет:

1. Что 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.

2. Обязательным является соблюдение конфиденциальности информации, доступ к которой ограничен федеральными законами.

3. Порядок идентификации информационных ресурсов в целях принятия мер по ограничению доступа к информационным ресурсам, требования к способам (методам) ограничения такого доступа, применяемым в соответствии с настоящим Федеральным законом, а также требования к размещаемой информации об ограничении доступа к информационным ресурсам определяются федеральным органом исполнительной власти, осуществляющим функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи.

4. Защита информации, составляющей государственную тайну, осуществляется в соответствии с законодательством Российской Федерации о государственной тайне.

5. Федеральными законами устанавливаются условия отнесения информации к сведениям, составляющим коммерческую тайну, служебную тайну и иную тайну, обязательность соблюдения конфиденциальности такой информации, а также ответственность за ее разглашение.

6. Информация, полученная гражданами (физическими лицами) при исполнении ими профессиональных обязанностей или организациями при осуществлении ими определенных видов деятельности (профессиональная тайна), подлежит защите в случаях, если на эти лица федеральными законами возложены обязанности по соблюдению конфиденциальности такой информации.

7. Информация, составляющая профессиональную тайну, может быть предоставлена третьим лицам в соответствии с федеральными законами и (или) по решению суда.

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

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

10. Порядок доступа к персональным данным граждан (физических лиц) устанавливается федеральным законом о персональных данных.

Правовое регулирование отношений, возникающих в сфере информации, информационных технологий и защиты информации, основывается на следующих принципах:

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

2) установление ограничений доступа к информации только федеральными законами;

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

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

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

6) достоверность информации и своевременность ее предоставления;

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

8) 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.

Информация, в зависимости от порядка ее предоставления или распространения, подразделяется на:

1) информацию, свободно распространяемую;

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

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

4) информацию, распространение которой в Российской Федерации ограничивается или запрещается.

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

Обладатель информации, если иное не предусмотрено федеральными законами, *вправе*:

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

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

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

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

5) осуществлять иные действия с информацией или разрешать осуществление таких действий.

Обладатель информации при осуществлении своих прав обязан:

1) соблюдать права и законные интересы иных лиц;

2) принимать меры по защите информации;

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

К общедоступной информации относятся общеизвестные сведения и иная информация, доступ к которой не ограничен.

Информация, размещаемая ее обладателями в сети Интернет в формате, допускающем автоматизированную обработку без предварительных изменений человеком в целях повторного ее использования, является общедоступной информацией, размещаемой в форме открытых данных.

Информация в форме открытых данных размещается в сети Интернет с учетом требований законодательства Российской Федерации о государственной тайне. В случае если размещение информации в форме открытых данных может привести к распространению сведений, составляющих государственную тайну, размещение указанной информации в форме открытых данных должно быть прекращено по требованию органа, наделенного полномочиями по распоряжению такими сведениями.

В случае если размещение информации в форме открытых данных может повлечь за собой нарушение прав обладателей информации, доступ к которой ограничен в соответствии с федеральными законами, или нарушение прав субъектов персональных данных, размещение указанной информации в форме открытых данных должно быть прекращено по решению суда. В случае если размещение информации в форме открытых данных осуществляется с нарушением требований Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», размещение информации в форме открытых данных должно быть приостановлено или прекращено по требованию уполномоченного органа по защите прав субъектов персональных данных.

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 настоящим Федеральным законом и другими федеральными законами.

Не может быть ограничен доступ к:

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

2) информации о состоянии окружающей среды;

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

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

5) информации, содержащейся в архивных документах архивных фондов (за исключением сведений и документов, доступ к которым ограничен законодательством Российской Федерации);

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

Предоставляется бесплатно информация:

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

2) затрагивающая права и установленные законодательством Российской Федерации обязанности заинтересованного лица;

3) иная установленная законом информация.

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.

Порядок идентификации информационных ресурсов в целях принятия мер по ограничению доступа к информационным ресурсам, требования к способам (методам) ограничения такого доступа, применяемым в соответствии с настоящим Федеральным законом, а также требования к размещаемой информации об ограничении доступа к информационным ресурсам определяются федеральным органом исполнительной власти, осуществляющим функции по

контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи.

Защита информации, составляющей государственную тайну, осуществляется в соответствии с законодательством Российской Федерации о государственной тайне.

Федеральными законами устанавливаются условия отнесения информации к сведениям, составляющим коммерческую тайну, служебную тайну и иную тайну, обязательность соблюдения конфиденциальности такой информации, а также ответственность за ее разглашение:

– информация, полученная гражданами (физическими лицами) при исполнении ими профессиональных обязанностей или организациями при осуществлении ими определенных видов деятельности (профессиональная тайна), подлежит защите в случаях, если на эти лица федеральными законами возложены обязанности по соблюдению конфиденциальности такой информации;

– информация, составляющая профессиональную тайну, может быть предоставлена третьим лицам в соответствии с федеральными законами и (или) по решению суда;

– срок исполнения обязанностей по соблюдению конфиденциальности информации, составляющей профессиональную тайну, может быть ограничен только с согласия гражданина (физического лица), предоставившего такую информацию о себе;

– запрещается требовать от гражданина (физического лица) предоставления информации о его частной жизни, в том числе информации, составляющей личную или семейную тайну, и получать такую информацию помимо воли гражданина (физического лица), если иное не предусмотрено федеральными законами.

Порядок доступа к персональным данным граждан (физических лиц) устанавливается федеральным законом о персональных данных.

С целью защиты сведений конфиденциального характера в Российской Федерации разработана система документов по конкретным сведениям, которые определенны Указом Президента Российской Федерации.

5.3. Персональные данные

Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

Федеральным законом «О персональных данных» от 27.07.2006 № 152-ФЗ регулируются отношения, связанные с обработкой персональных данных, осуществляемой федеральными органами государственной власти, органами государственной власти субъектов Российской Федерации, иными государственными органами (далее – государственные органы), органами местного самоуправления, иными муниципальными органами (далее – муниципальные органы), юридическими лицами и физическими лицами с использованием средств автоматизации, в том числе в информационно-телекоммуникационных сетях, или без использования таких средств, если обработка персональных данных без использования таких средств соответствует характеру действий (операций), совершаемых с персональными данными с использованием средств автоматизации, то есть позволяет осуществлять в соответствии с заданным алгоритмом поиск персональных данных, зафиксированных на материальном носителе и содержащихся в картотеках или иных систематизированных собраниях персональных данных, и (или) доступ к таким персональным данным (рис. 5.1).

Действие закона не распространяется на отношения, возникающие при:

1) обработке персональных данных физическими лицами исключительно для личных и семейных нужд, если при этом не нарушаются права субъектов персональных данных;

2) организации хранения, комплектования, учета и использования содержащих персональные данные документов Архивного фонда Российской Федерации и других архивных документов в соответствии с законодательством об архивном деле в Российской Федерации;

3) обработке персональных данных, отнесенных в установленном порядке к сведениям, составляющим государственную тайну.

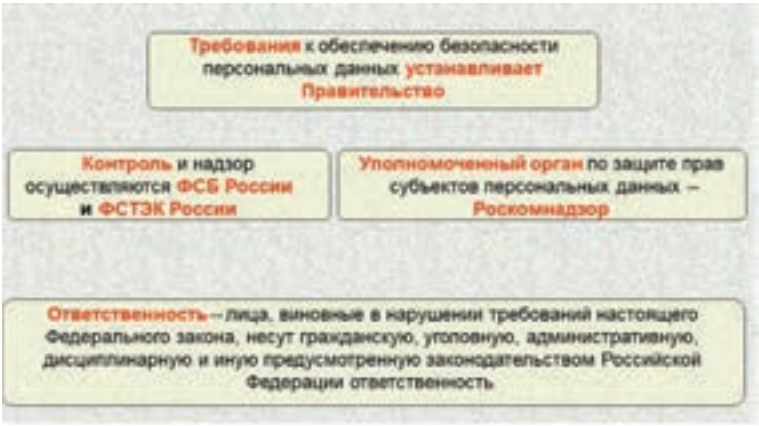

Рис. 5.1. Организация защиты персональных данных

Целью настоящего Федерального закона является обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну.

5.3.1. Законодательство Российской Федерации в области персональных данных

Законодательство Российской Федерации в области персональных данных основывается на Конституции Российской Федерации и международных договорах Российской Федерации и состоит из Федерального закона «О персональных данных» и других определяющих случаи и особенности обработки персональных данных федеральных законов.

На основании и во исполнение федеральных законов государственные органы, Банк России, органы местного самоуправления в пределах своих полномочий могут принимать нормативные правовые акты, нормативные акты, правовые акты по отдельным вопросам, касающимся обработки персональных данных. Такие акты не могут содержать положения, ограничивающие права субъектов персональных данных, устанавливающие не предусмотренные федеральными законами ограничения деятельности операторов или

возлагающие на операторов не предусмотренные федеральными законами обязанности, и подлежат официальному опубликованию.

Особенности обработки персональных данных, осуществляемой без использования средств автоматизации, могут быть установлены федеральными законами и иными нормативными правовыми актами Российской Федерации с учетом положений настоящего Федерального закона.

Если международным договором Российской Федерации установлены иные правила, чем те, которые предусмотрены настоящим Федеральным законом, применяются правила международного договора.

5.3.2. Принципы и условия обработки персональных данных

К принципам обработки персональных данных относятся (рис. 5.2):

1. Обработка персональных данных должна осуществляться на законной и справедливой основе.

2. Обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных.

3. Не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой.

4. Обработке подлежат только персональные данные, которые отвечают целям их обработки.

5. Содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки. Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки.

6. При обработке персональных данных должны быть обеспечены точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных. Оператор должен принимать необходимые меры либо обеспечивать их принятие по удалению или уточнению неполных или неточных данных.

Рис. 5.2. Принципы и условия обработки персональных данных

7. Хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных. Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

5.3.3. Условия обработки персональных данных

Обработка персональных данных допускается в следующих случаях:

1) обработка персональных данных осуществляется с согласия субъекта персональных данных на обработку его персональных данных;

2) обработка персональных данных необходима для достижения целей, предусмотренных международным договором Российской Федерации или законом, для осуществления и выполнения возложенных законодательством Российской Федерации на оператора функций, полномочий и обязанностей;

3) обработка персональных данных осуществляется в связи с участием лица в конституционном, гражданском, административном, уголовном судопроизводстве, судопроизводстве в арбитражных судах;

4) обработка персональных данных необходима для исполнения судебного акта, акта другого органа или должностного лица, подлежащих исполнению в соответствии с законодательством Российской Федерации об исполнительном производстве;

5) обработка персональных данных необходима для исполнения полномочий федеральных органов исполнительной власти, органов государственных внебюджетных фондов, исполнительных органов государственной власти субъектов Российской Федерации, органов местного самоуправления и функций организаций, участвующих в предоставлении, соответственно, государственных и муниципальных услуг, предусмотренных Федеральным законом от 27 июля 2010 г. № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг», включая регистрацию субъекта персональных данных на едином портале государственных и муниципальных услуг и (или) региональных порталах государственных и муниципальных услуг;

6) обработка персональных данных необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных, а также для заключения договора по инициативе субъекта персональных данных или договора, по которому субъект персональных данных будет являться выгодоприобретателем или поручителем;

7) обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта

персональных данных, если получение согласия субъекта персональных данных невозможно;

8) обработка персональных данных необходима для осуществления прав и законных интересов оператора или третьих лиц, в том числе в случаях, предусмотренных Федеральным законом «О защите прав и законных интересов физических лиц при осуществлении деятельности по возврату просроченной задолженности и о внесении изменений в Федеральный закон «О микрофинансовой деятельности и микрофинансовых организациях», либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта персональных данных;

9) обработка персональных данных необходима для осуществления профессиональной деятельности журналиста и (или) законной деятельности средства массовой информации либо научной, литературной или иной творческой деятельности при условии, что при этом не нарушаются права и законные интересы субъекта персональных данных;

10) обработка персональных данных осуществляется в статистических или иных исследовательских целях, за исключением использования в целях продвижения товаров, работ, услуг на рынке, а также в целях политической агитации, при условии обязательного обезличивания персональных данных;

11) осуществляется обработка персональных данных, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных либо по его просьбе;

12) осуществляется обработка персональных данных, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральным законом.

13) Обработка персональных данных объектов государственной охраны и членов их семей осуществляется с учетом особенностей, предусмотренных Федеральным законом от 27.05.1996 № 57-ФЗ «О государственной охране»:

Документы и материалы, содержащие сведения о кадровом составе органов государственной охраны, о лицах, оказывающих или оказывавших им содействие на конфиденциальной основе, а также об организации, о тактике, методах и средствах осуществления

деятельности органов государственной охраны, подлежат хранению в архиве федерального органа исполнительной власти в области государственной охраны.

14. Оператор вправе поручить обработку персональных данных другому лицу с согласия субъекта персональных данных, если иное не предусмотрено федеральным законом, на основании заключаемого с этим лицом договора, в том числе государственного или муниципального контракта, либо путем принятия государственным или муниципальным органом соответствующего акта (далее – поручение оператора). Лицо, осуществляющее обработку персональных данных по поручению оператора, обязано соблюдать принципы и правила обработки персональных данных, предусмотренные настоящим Федеральным законом. В поручении оператора должны быть определены перечень действий (операций) с персональными данными, которые будут совершаться лицом, осуществляющим обработку персональных данных, и цели обработки, должна быть установлена обязанность такого лица соблюдать конфиденциальность персональных данных и обеспечивать безопасность персональных данных при их обработке, а также должны быть указаны требования к защите обрабатываемых персональных данных.

15. Лицо, осуществляющее обработку персональных данных по поручению оператора, не обязано получать согласие субъекта персональных данных на обработку его персональных данных.

16. Если оператор поручает обработку персональных данных другому лицу, ответственность перед субъектом персональных данных за действия указанного лица несет оператор. Лицо, осуществляющее обработку персональных данных по поручению оператора, несет ответственность перед оператором.

5.3.4. Общедоступные источники персональных данных

1. В целях информационного обеспечения могут создаваться общедоступные источники персональных данных (в том числе справочники, адресные книги). В общедоступные источники персональных данных с письменного согласия субъекта персональных данных могут включаться его фамилия, имя, отчество, год и место

рождения, адрес, абонентский номер, сведения о профессии и иные персональные данные, сообщаемые субъектом персональных данных.

2. Сведения о субъекте персональных данных должны быть в любое время исключены из общедоступных источников персональных данных по требованию субъекта персональных данных либо по решению суда или иных уполномоченных государственных органов.

5.3.5. Согласие субъекта персональных данных на обработку его персональных данных

1. Субъект персональных данных принимает решение о предоставлении его персональных данных и дает согласие на их обработку свободно, своей волей и в своем интересе (рис. 5.3). Согласие на обработку персональных данных должно быть конкретным, информированным и сознательным. Согласие на обработку персональных данных может быть дано субъектом персональных данных или его представителем в любой позволяющей подтвердить факт его получения форме, если иное не установлено федеральным законом. В случае получения согласия на обработку персональных данных от представителя субъекта персональных данных полномочия данного представителя на дачу согласия от имени субъекта персональных данных проверяются оператором.

2. Согласие на обработку персональных данных может быть отозвано субъектом персональных данных. В случае отзыва субъектом персональных данных согласия на обработку персональных данных оператор вправе продолжить обработку персональных данных без согласия субъекта персональных данных при наличии оснований, указанных в законе.

3. Обязанность предоставить доказательство получения согласия субъекта персональных данных на обработку его персональных данных или доказательство наличия оснований, указанных в законе, возлагается на оператора.

4. В случаях, предусмотренных федеральным законом, обработка персональных данных осуществляется только с согласия в письменной форме субъекта персональных данных. Равнозначным

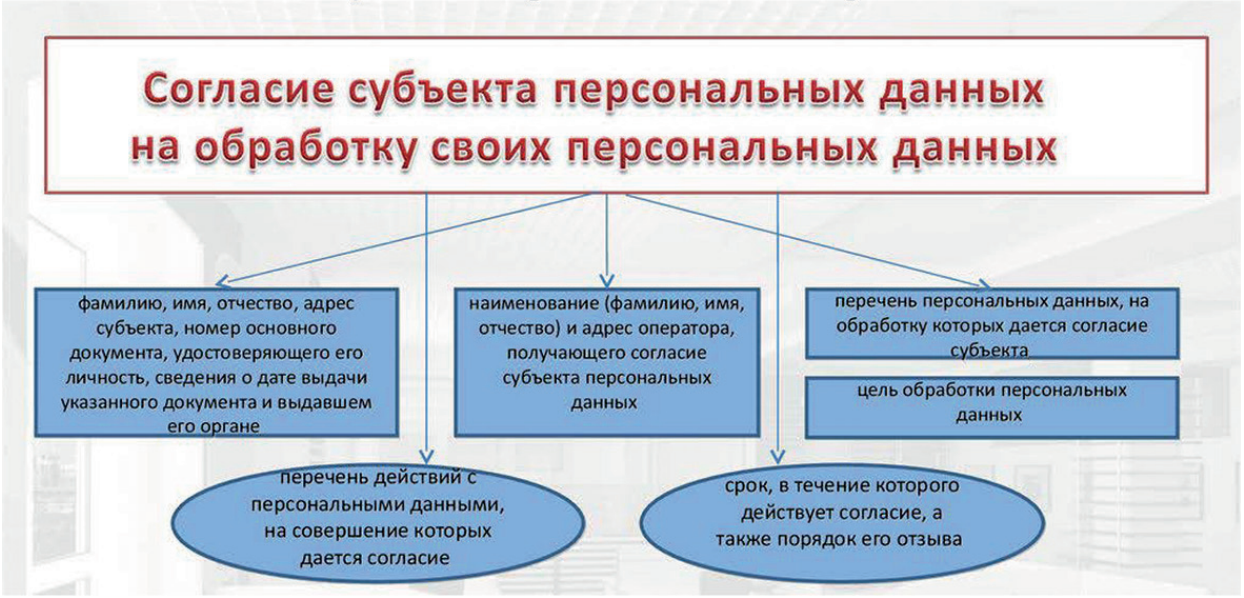

Рис. 5.3. Согласие на обработку персональных данных

содержащему собственноручную подпись субъекта персональных данных согласию в письменной форме на бумажном носителе признается согласие в форме электронного документа, подписанного в соответствии с федеральным законом электронной подписью. Согласие в письменной форме субъекта персональных данных на обработку его персональных данных должно включать в себя, в частности:

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

2) фамилию, имя, отчество, адрес представителя субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе, реквизиты доверенности или иного документа, подтверждающего полномочия этого представителя (при получении согласия от представителя субъекта персональных данных);

3) наименование или фамилию, имя, отчество и адрес оператора, получающего согласие субъекта персональных данных;

4) цель обработки персональных данных;

5) перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;

6) наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка будет поручена такому лицу;

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

8) срок, в течение которого действует согласие субъекта персональных данных, а также способ его отзыва, если иное не установлено федеральным законом;

9) подпись субъекта персональных данных.

5. Порядок получения в форме электронного документа согласия субъекта персональных данных на обработку его персональных данных в целях предоставления государственных и муниципальных услуг, а также услуг, которые являются необходимыми

и обязательными для предоставления государственных и муниципальных услуг, устанавливается Правительством Российской Федерации.

6. В случае недееспособности субъекта персональных данных согласие на обработку его персональных данных дает законный представитель субъекта персональных данных.

7. В случае смерти субъекта персональных данных согласие на обработку его персональных данных дают наследники субъекта персональных данных, если такое согласие не было дано субъектом персональных данных при его жизни.

5.3.6. Специальные категории персональных данных

Обработка специальных категорий персональных данных (рис. 5.4), касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни, не допускается, за исключением случаев:

– субъект персональных данных дал согласие в письменной форме на обработку своих персональных данных;

– персональные данные сделаны общедоступными субъектом персональных данных;

– обработка персональных данных необходима в связи с реализацией международных договоров Российской Федерации о реадмиссии;

– обработка персональных данных осуществляется в соответствии с Федеральным законом от 25 января 2002 г. № 8-ФЗ «О Всероссийской переписи населения»;

– обработка персональных данных осуществляется в соответствии с законодательством о государственной социальной помощи, трудовым законодательством, пенсионным законодательством Российской Федерации;

– обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных либо жизни, здоровья или иных жизненно важных интересов других лиц и получение согласия субъекта персональных данных невозможно;

Рис. 5.4. Специальная категория персональных данных

– обработка персональных данных осуществляется в медико-профилактических целях, в целях установления медицинского диагноза, оказания медицинских и медико-социальных услуг при условии, что обработка персональных данных осуществляется лицом, профессионально занимающимся медицинской деятельностью и обязанным в соответствии с законодательством Российской Федерации сохранять врачебную тайну;

– обработка персональных данных членов (участников) общественного объединения или религиозной организации осуществляется соответствующими общественным объединением или религиозной организацией, действующими в соответствии с законодательством Российской Федерации, для достижения законных целей, предусмотренных их учредительными документами, при условии, что персональные данные не будут распространяться без согласия в письменной форме субъектов персональных данных;

– обработка персональных данных необходима для установления или осуществления прав субъекта персональных данных или третьих лиц, а равно и в связи с осуществлением правосудия;

– обработка персональных данных осуществляется в соответствии с законодательством Российской Федерации об обороне, о безопасности, о противодействии терроризму, о транспортной

безопасности, о противодействии коррупции, об оперативно-разыскной деятельности, об исполнительном производстве, уголовно-исполнительным законодательством Российской Федерации;

– обработка полученных в установленных законодательством Российской Федерации случаях персональных данных осуществляется органами прокуратуры в связи с осуществлением ими прокурорского надзора;

– обработка персональных данных осуществляется в соответствии с законодательством об обязательных видах страхования, со страховым законодательством;

– обработка персональных данных осуществляется в случаях, предусмотренных законодательством Российской Федерации, государственными органами, муниципальными органами или организациями в целях устройства детей, оставшихся без попечения родителей, на воспитание в семьи граждан;

– обработка персональных данных осуществляется в соответствии с законодательством Российской Федерации о гражданстве Российской Федерации.

Обработка персональных данных о судимости может осуществляться государственными органами или муниципальными органами в пределах полномочий, предоставленных им в соответствии с законодательством Российской Федерации, а также иными лицами в случаях и в порядке, которые определяются в соответствии с федеральными законами.

Обработка специальных категорий персональных данных, осуществлявшаяся в случаях, предусмотренных ч. 2 и 3 настоящей статьи, должна быть незамедлительно прекращена, если устранены причины, вследствие которых осуществлялась обработка, если иное не установлено федеральным законом.

5.3.7. Биометрические персональные данные

Сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность (биометрические персональные данные) (рис. 5.5) и которые используются оператором для установления личности субъекта персональных данных, могут обрабатываться

Рис. 5.5. Понятия биометрических данных

только при наличии согласия в письменной форме субъекта персональных данных, за исключением случаев, предусмотренных ч. 2 настоящей статьи.

Обработка биометрических персональных данных может осуществляться без согласия субъекта персональных данных в связи с реализацией международных договоров Российской Федерации о реадмиссии, в связи с осуществлением правосудия и исполнением судебных актов, в связи с проведением обязательной государственной дактилоскопической регистрации, а также в случаях, предусмотренных законодательством Российской Федерации об обороне, о безопасности, о противодействии терроризму, о транспортной безопасности, о противодействии коррупции, об оперативно-разыскной деятельности, о государственной службе, уголовно-исполнительным законодательством Российской Федерации, законодательством Российской Федерации о порядке выезда из Российской Федерации и въезда в Российскую Федерацию, о гражданстве Российской Федерации.

5.3.8. Обязанности оператора при сборе персональных данных

До начала обработки персональных данных обязан предоставить субъекту персональных данных следующую информацию:

– наименование либо фамилия, имя, отчество и адрес оператора или его представителя;

– цель обработки персональных данных и ее правовое основание;

– предполагаемые пользователи персональных данных;

– установленные настоящим Федеральным законом права субъекта персональных данных;

– источник получения персональных данных.

Оператор освобождается от обязанности предоставить субъекту персональных данных сведения, в случаях если:

– субъект персональных данных уведомлен об осуществлении обработки его персональных данных соответствующим оператором;

– персональные данные получены оператором на основании федерального закона или в связи с исполнением договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных;

– персональные данные сделаны общедоступными субъектом персональных данных или получены из общедоступного источника;

– оператор осуществляет обработку персональных данных для статистических или иных исследовательских целей, для осуществления профессиональной деятельности журналиста либо научной, литературной или иной творческой деятельности, если при этом не нарушаются права и законные интересы субъекта персональных данных;

– предоставление субъекту персональных данных сведений нарушает права и законные интересы третьих лиц.

При сборе персональных данных, в том числе посредством информационно-телекоммуникационной сети Интернет, оператор обязан обеспечить запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации с использованием баз данных, находящихся на территории Российской Федерации.

5.3.9. Меры по обеспечению безопасности персональных данных при их обработке

Оператор при обработке персональных данных (рис. 5.6) обязан принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

Обеспечение безопасности персональных данных достигается, в частности:

1) определением угроз безопасности персональных данных при их обработке в информационных системах персональных данных;

2) применением организационных и технических мер по обеспечению безопасности персональных данных при их обработке

Рис. 5.6. Действия оператора при работе с персональными данными

в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных;

3) применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;

4) оценкой эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;

5) учетом машинных носителей персональных данных;

6) обнаружением фактов несанкционированного доступа к персональным данным и принятием мер;

7) восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

8) установлением правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных;

9) контролем за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных.

5.3.10. Лица, ответственные за организацию обработки персональных данных в организациях

1. Оператор, являющийся юридическим лицом, назначает лицо, ответственное за организацию обработки персональных данных.

2. Лицо, ответственное за организацию обработки персональных данных, получает указания непосредственно от исполнительного органа организации, являющейся оператором, и подотчетно ему.

3. Лицо, ответственное за организацию обработки персональных данных, в частности, обязано:

1) осуществлять внутренний контроль за соблюдением оператором и его работниками законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных;

2) доводить до сведения работников оператора положения законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных;

3) организовывать прием и обработку обращений и запросов субъектов персональных данных или их представителей и (или) осуществлять контроль за приемом и обработкой таких обращений и запросов.

4. Финансирование уполномоченного органа по защите прав субъектов персональных данных осуществляется за счет средств федерального бюджета.

5. При уполномоченном органе по защите прав субъектов персональных данных создается на общественных началах консультативный совет, порядок формирования и порядок деятельности которого определяются уполномоченным органом по защите прав субъектов персональных данных.

5.3.11. Ответственность за нарушение требований Федерального закона «О персональных данных»

Лица, виновные в нарушении требований настоящего Федерального закона, несут предусмотренную законодательством Российской Федерации ответственность (рис. 5.7).

Моральный вред, причиненный субъекту персональных данных вследствие нарушения его прав, нарушения правил обработки персональных данных, установленных настоящим Федеральным законом, а также требований к защите персональных данных, установленных в соответствии с настоящим Федеральным законом, подлежит возмещению в соответствии с законодательством Российской Федерации. Возмещение морального вреда осуществляется независимо от возмещения имущественного вреда и понесенных субъектом персональных данных убытков.

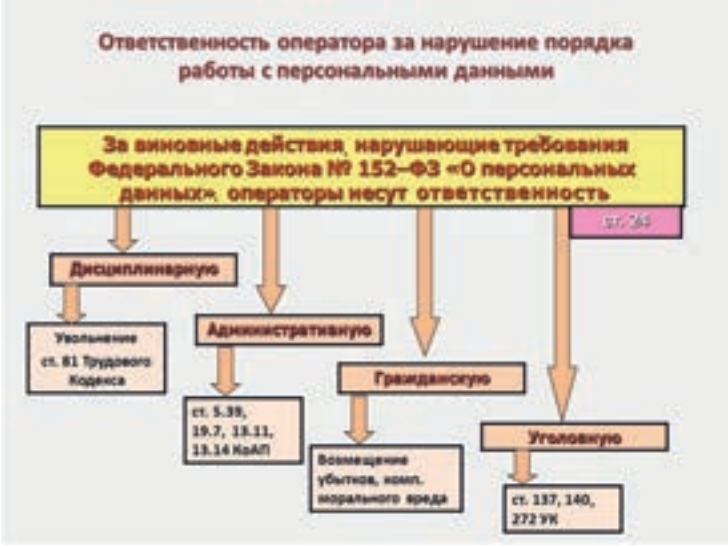

Рис. 5.7. Ответственность за нарушение закона «О персональных данных»

5.4. Тайна следствия и судопроизводства

Предоставление, распространение, передача и получение информации о деятельности судов в Российской Федерации, содержащей персональные данные, ведение и использование информационных систем и информационно-телекоммуникационных сетей в целях создания условий для доступа к указанной информации осуществляются в соответствии с Федеральным законом от 22 декабря 2008 г. № 262-ФЗ «Об обеспечении доступа к информации о деятельности судов в Российской Федерации».

В соответствии со ст. 161 Уголовно-процессуального кодекса Российской Федерации от 18.12.2001 № 174-ФЗ определена недопустимость разглашения данных предварительного расследования, а именно:

1. Данные предварительного расследования не подлежат разглашению, за исключением случаев, предусмотренных ч. 2, 4 и 6 настоящей статьи.

2. Данные предварительного расследования могут быть преданы гласности лишь с разрешения следователя или дознавателя, и только в том объеме, в каком ими будет признано это допустимым, если разглашение не противоречит интересам предварительного расследования и не связано с нарушением прав, свобод и законных интересов участников уголовного судопроизводства.

3. Следователь или дознаватель предупреждает участников уголовного судопроизводства о недопустимости разглашения без соответствующего разрешения данных предварительного расследования, о чем у них берется подписка с предупреждением об ответственности в соответствии со ст. 310 Уголовного кодекса Российской Федерации.

5.5. Служебная тайна

Основной руководящий документ по защите служебной тайны – Постановление Правительства РФ от 3.11.1994 № 1233 «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти, уполномоченном органе управления использованием атомной энергии и уполномоченном органе по космической деятельности».

5.5.1. Общие положения

Положение определяет общий порядок обращения с документами и другими материальными носителями информации, содержащими служебную информацию ограниченного распространения, в федеральных органах исполнительной власти, уполномоченном органе управления использованием атомной энергии и уполномоченном органе по космической деятельности, а также на подведомственных им предприятиях, в учреждениях и организациях.

Положение не распространяется на порядок обращения с документами, содержащими сведения, составляющие государственную тайну.

К служебной информации ограниченного распространения относится несекретная информация, касающаяся деятельности

организаций, ограничения на распространение которой диктуются служебной необходимостью, а также поступившая в организации несекретная информация, доступ к которой ограничен в соответствии с федеральными законами.

Не могут быть отнесены к служебной информации ограниченного распространения:

– акты законодательства, устанавливающие правовой статус государственных органов, организаций, общественных объединений, а также права, свободы и обязанности граждан, порядок их реализации;

– сведения о чрезвычайных ситуациях, опасных природных явлениях и процессах, экологическая, гидрометеорологическая, гидрогеологическая, демографическая, санитарно-эпидемиологическая и другая информация, необходимая для обеспечения безопасного существования населенных пунктов, граждан и населения в целом, а также производственных объектов;

– описание структуры органа исполнительной власти, его функций, направлений и форм деятельности, а также его адрес;

– порядок рассмотрения и разрешения заявлений, а также обращений граждан и юридических лиц;

– решения по заявлениям и обращениям граждан и юридических лиц, рассмотренным в установленном порядке;

– сведения об исполнении бюджета и использовании других государственных ресурсов, о состоянии экономики и потребностей населения;

– документы, накапливаемые в открытых фондах библиотек и архивов, информационных системах организаций, необходимые для реализации прав, свобод и обязанностей граждан.

На документах (в необходимых случаях и на их проектах), содержащих служебную информацию ограниченного распространения, проставляется пометка «Для служебного пользования».

Руководитель федерального органа исполнительной власти, уполномоченного органа управления использованием атомной энергии, уполномоченного органа по космической деятельности в пределах своей компетенции определяет:

– категории должностных лиц, уполномоченных относить служебную информацию к разряду ограниченного распространения;

– порядок передачи служебной информации ограниченного распространения другим органам и организациям;

– порядок снятия пометки «Для служебного пользования» с носителей информации ограниченного распространения;

– организацию защиты служебной информации ограниченного распространения.

Должностные лица, принявшие решение об отнесении служебной информации к разряду ограниченного распространения, несут персональную ответственность за обоснованность принятого решения и за соблюдение ограничений, предусмотренных Положением.

Служебная информация ограниченного распространения без санкции соответствующего должностного лица не подлежит разглашению (распространению).

За разглашение служебной информации ограниченного распространения, а также нарушение порядка обращения с документами, содержащими такую информацию, государственный служащий (работник организации) может быть привлечен к дисциплинарной или иной предусмотренной законодательством ответственности.

В случае ликвидации федерального органа исполнительной власти, уполномоченного органа управления использованием атомной энергии, уполномоченного органа по космической деятельности, организации решение о дальнейшем использовании служебной информации ограниченного распространения принимает ликвидационная комиссия.

5.5.2. Порядок обращения с документами, содержащими служебную информацию ограниченного распространения

Необходимость проставления пометки «Для служебного пользования» на документах и изданиях, содержащих служебную информацию ограниченного распространения, определяется исполнителем и должностным лицом, подписывающим или утверждающим документ. Указанная пометка и номер экземпляра

проставляются в правом верхнем углу первой страницы документа, на обложке и титульном листе издания, а также на первой странице сопроводительного письма к таким документам.

Прием и учет (регистрация) документов, содержащих служебную информацию ограниченного распространения, осуществляются, как правило, структурными подразделениями, которым поручен прием и учет несекретной документации.

Документы с пометкой «Для служебного пользования»:

– печатаются в машинописном бюро. На обороте последнего листа каждого экземпляра документа машинистка должна указать количество отпечатанных экземпляров, фамилию исполнителя, свою фамилию и дату печатания документа. Отпечатанные и подписанные документы вместе с черновиками и вариантами передаются для регистрации работнику, осуществляющему их учет. Черновики и варианты уничтожаются этим работником с отражением факта уничтожения в учетных формах;

– учитываются, как правило, отдельно от несекретной документации. При незначительном объеме таких документов разрешается вести их учет совместно с другими несекретными документами. К регистрационному индексу документа добавляется пометка «ДСП»;

– передаются работникам подразделений под расписку;

– пересылаются сторонним организациям фельдъегерской связью, заказными или ценными почтовыми отправлениями;

– размножаются (тиражируются) только с письменного разрешения соответствующего руководителя. Учет размноженных документов осуществляется поэкземплярно;

– хранятся в надежно запираемых и опечатываемых шкафах (ящиках, хранилищах).

При необходимости направления документов с пометкой «Для служебного пользования» в несколько адресов составляется указатель рассылки, в котором поадресно проставляются номера экземпляров отправляемых документов. Указатель рассылки подписывается исполнителем и руководителем структурного подразделения, готовившего документ.

Исполненные документы с пометкой «Для служебного пользования» группируются в дела в соответствии с номенклатурой дел несекретного делопроизводства. При этом на обложке дела, в которое помещены такие документы, также проставляется пометка «Для служебного пользования».

Уничтожение дел, документов с пометкой «Для служебного пользования», утративших свое практическое значение и не имеющих исторической ценности, производится по акту. В учетных формах об этом делается отметка со ссылкой на соответствующий акт.

Передача документов и дел с пометкой «Для служебного пользования» от одного работника другому осуществляется с разрешения соответствующего руководителя.

При смене работника, ответственного за учет документов с пометкой «Для служебного пользования», составляется акт приема-передачи этих документов, который утверждается соответствующим руководителем.

Проверка наличия документов, дел и изданий с пометкой «Для служебного пользования» проводится не реже одного раза в год комиссиями, назначаемыми приказом руководителя. В состав таких комиссий обязательно включаются работники, ответственные за учет и хранение этих материалов.

В библиотеках и архивах, где сосредоточено большое количество изданий, дел и других материалов с пометкой «Для служебного пользования», проверка наличия может проводиться не реже одного раза в пять лет.

Результаты проверки оформляются актом.

О фактах утраты документов, дел и изданий, содержащих служебную информацию ограниченного распространения, либо разглашения этой информации ставится в известность руководитель организации и назначается комиссия для расследования обстоятельств утраты или разглашения. Результаты расследования докладываются руководителю, назначившему комиссию.

На утраченные документы, дела и издания с пометкой «Для служебного пользования» составляется акт, на основании которого делаются соответствующие отметки в учетных формах. Акты на

утраченные дела постоянного срока хранения после их утверждения передаются в архив для включения в дело фонда.

При снятии пометки «Для служебного пользования» на документах, делах или изданиях, а также в учетных формах делаются соответствующие отметки и информируются все адресаты, которым эти документы (издания) направлялись.

Органы государственной власти предусматривают законодательно защиту сведений конфиденциального характера, к примеру в ст. 17. Защита сведений об органах государственной охраны Федерального закона от 27.05.1996 № 57-ФЗ «О государственной охране» говорится:

Документы и материалы, содержащие сведения о кадровом составе органов государственной охраны, о лицах, оказывающих или оказывавших им содействие на конфиденциальной основе, а также об организации, о тактике, методах и средствах осуществления деятельности органов государственной охраны, подлежат хранению в архиве федерального органа исполнительной власти в области государственной охраны.

Материалы архива федерального органа исполнительной власти в области государственной охраны, представляющие историческую и научную ценность, рассекреченные в соответствии с федеральным законодательством, передаются на хранение в архивы уполномоченного федерального органа исполнительной власти в сфере архивного дела и делопроизводства в порядке, установленном федеральным законодательством.

5.6. Врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных, иных сообщений

5.6.1. Соблюдение врачебной тайны

Соблюдение врачебной тайны определено в ст. 13. Федерального закона от 21.11.2011 № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации»:

1. Сведения о факте обращения гражданина за оказанием медицинской помощи, состоянии его здоровья и диагнозе, иные сведения, полученные при его медицинском обследовании и лечении, составляют врачебную тайну.

2. Не допускается разглашение сведений, составляющих врачебную тайну, в том числе после смерти человека, лицами, которым они стали известны при обучении, исполнении трудовых, должностных, служебных и иных обязанностей, за исключением случаев, установленных ч. 3 и 4 настоящей статьи.

3. С письменного согласия гражданина или его законного представителя допускается разглашение сведений, составляющих врачебную тайну, другим гражданам, в том числе должностным лицам, в целях медицинского обследования и лечения пациента, проведения научных исследований, их опубликования в научных изданиях, использования в учебном процессе и в иных целях.

4. Предоставление сведений, составляющих врачебную тайну, без согласия гражданина или его законного представителя допускается:

– в целях проведения медицинского обследования и лечения гражданина, который в результате своего состояния не способен выразить свою волю, с учетом положений п. 1 ч. 9 ст. 20 Федерального закона;

– при угрозе распространения инфекционных заболеваний, массовых отравлений и поражений;

– по запросу органов дознания и следствия, суда в связи с проведением расследования или судебным разбирательством, по запросу органов прокуратуры в связи с осуществлением ими прокурорского надзора, по запросу органа уголовно-исполнительной системы в связи с исполнением уголовного наказания и осуществлением контроля за поведением условно осужденного, осужденного, в отношении которого отбывание наказания отсрочено, и лица, освобожденного условно досрочно, а также в связи с исполнением осужденным обязанности пройти лечение от наркомании и медицинскую и (или) социальную реабилитацию;

– в целях осуществления уполномоченными федеральными органами исполнительной власти контроля за исполнением лицами, признанными больными наркоманией, либо потребляющими наркотические средства или психотропные вещества без назначения врача, либо новые потенциально опасные психоактивные вещества, возложенной на них при назначении административного наказания судом обязанности пройти лечение от наркомании, диагностику, профилактические мероприятия и (или) медицинскую реабилитацию;

– в случае оказания медицинской помощи несовершеннолетнему, в соответствии с п. 2 ч. 2 ст. 20 Федерального закона, а также несовершеннолетнему, не достигшему возраста, установленного ч. 2 ст. 54 Федерального закона, для информирования одного из его родителей или иного законного представителя;

– в целях информирования органов внутренних дел о поступлении пациента, в отношении которого имеются достаточные основания полагать, что вред его здоровью причинен в результате противоправных действий;

– в целях проведения военно-врачебной экспертизы по запросам военных комиссариатов, кадровых служб и военно-врачебных (врачебно-летных) комиссий федеральных органов исполнительной власти и федеральных государственных органов, в которых федеральным законом предусмотрена военная и приравненная к ней служба;

– в целях расследования несчастного случая на производстве и профессионального заболевания, а также несчастного случая с обучающимся во время пребывания в организации, осуществляющей образовательную деятельность, и в соответствии с ч. 6 ст. 34.1 Федерального закона от 4 декабря 2007 г. № 329-ФЗ «О физической культуре и спорте в Российской Федерации» несчастного случая с лицом, проходящим спортивную подготовку и не состоящим в трудовых отношениях с физкультурно-спортивной организацией, не осуществляющей спортивной подготовки и являющейся заказчиком услуг по спортивной подготовке, во время прохождения таким лицом спортивной подготовки в организации, осуществляющей

спортивную подготовку, в том числе во время его участия в спортивных соревнованиях, предусмотренных реализуемыми программами спортивной подготовки;

– при обмене информацией медицинскими организациями, в том числе размещенной в медицинских информационных системах, в целях оказания медицинской помощи с учетом требований законодательства Российской Федерации о персональных данных;

– в целях осуществления учета и контроля в системе обязательного социального страхования;

– в целях осуществления контроля качества и безопасности медицинской деятельности в соответствии с настоящим Федеральным законом.

5.6.2. Гарантии нотариальной деятельности

В ст. 5. «Основы законодательства Российской Федерации о нотариате» (утв. ВС РФ 11.02.1993 № 4462-1) определено (рис. 5.8):

1. Нотариус беспристрастен и независим в своей деятельности и руководствуется Конституцией Российской Федерации, конституциями (уставами) субъектов Российской Федерации, настоящими Основами, иными нормативными правовыми актами Российской Федерации и субъектов Российской Федерации, принятыми в пределах их компетенции, а также международными договорами.

2. Нотариусу при исполнении служебных обязанностей, лицу, замещающему временно отсутствующего нотариуса, а также лицам, работающим в нотариальной конторе, запрещается разглашать сведения, оглашать документы, которые стали им известны в связи с совершением нотариальных действий, в том числе и после сложения полномочий или увольнения, за исключением случаев, предусмотренных настоящими Основами.

3. Сведения (документы) о совершенных нотариальных действиях могут выдаваться только лицам, от имени или по поручению которых совершены эти действия, если иное не установлено настоящей статьей.

Рис. 5.8. Содержание нотариальной тайны

4. Сведения о совершенных нотариальных действиях выдаются по требованию суда, прокуратуры, органов следствия в связи с находящимися в их производстве уголовными, гражданскими или административными делами, а также по требованию судебных приставов-исполнителей в связи с находящимися в их производстве материалами по исполнению исполнительных документов, по запросам органа, осуществляющего государственную регистрацию юридических лиц и индивидуальных предпринимателей, в связи с государственной регистрацией и по запросам органов, предоставляющих государственные и муниципальные услуги и исполняющих государственные и муниципальные функции, в порядке, установленном ч. 5 ст. 34.4 настоящих Основ, и нотариусов в связи с совершаемыми нотариальными действиями. Справки о выдаче свидетельств о праве на наследство и о нотариальном удостоверении договоров дарения направляются в налоговый орган в случаях и в порядке, которые предусмотрены законодательством Российской Федерации о налогах и сборах. Справки о завещании выдаются только после смерти завещателя.

5. При совершении нотариальных действий согласие субъекта персональных данных на обработку его персональных данных для совершения нотариальных действий не требуется.

5.6.3. Адвокатская тайна

В ст. 8.Федерального закона от 31.05.2002 № 63-ФЗ «Об адвокатской деятельности и адвокатуре в Российской Федерации» определено:

1. Адвокатской тайной являются любые сведения, связанные с оказанием адвокатом юридической помощи своему доверителю.

2. Адвокат не может быть вызван и допрошен в качестве свидетеля об обстоятельствах, ставших ему известными в связи с обращением к нему за юридической помощью или в связи с ее оказанием.

3. Проведение оперативно-разыскных мероприятий и следственных действий в отношении адвоката (в том числе в жилых и служебных помещениях, используемых им для осуществления адвокатской деятельности) допускается только на основании судебного решения.

Полученные в ходе оперативно-разыскных мероприятий или следственных действий (в том числе после приостановления или прекращения статуса адвоката) сведения, предметы и документы могут быть использованы в качестве доказательств обвинения только в тех случаях, когда они не входят в производство адвоката по делам его доверителей. Указанные ограничения не распространяются на орудия преступления, а также на предметы, которые запрещены к обращению или оборот которых ограничен в соответствии с законодательством Российской Федерации.

5.6.4. Тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений

Статья 23 Конституции Российской Федерации определяет:

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

2. Каждый имеет право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений. Ограничение этого права допускается только на основании судебного решения.

Статья 13 Уголовно-процессуального кодекса Российской Федерации» от 18.12.2001 № 174-ФЗ определила в части тайны переписки, телефонных и иных переговоров, почтовых, телеграфных и иных сообщений:

1. Ограничение права гражданина на тайну переписки, телефонных и иных переговоров, почтовых, телеграфных и иных сообщений допускается только на основании судебного решения.

2. Наложение ареста на почтовые и телеграфные отправления и их выемка в учреждениях связи, контроль и запись телефонных и иных переговоров, получение информации о соединениях между абонентами и (или) абонентскими устройствами могут производиться только на основании судебного решения.

Верховный суд России разъяснил, при каких обстоятельствах суды должны считать нарушенными тайны переписки и переговоров:

«Тайна переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений признается нарушенной, когда доступ, как к их содержанию, так и к информации о самих фактах переписки, переговоров, сообщений, совершен без согласия лица, чью тайну они составляют», – говорится в проекте пленума Верховного суда. Нарушением тайны телефонных переговоров является незаконный доступ к данным о входящих и исходящих звонках. Речь идет в том числе и о времени, дате, продолжительности контакта, телефонных номерах и прочей информации, которая позволяет установить личность абонента.

При этом Верховный суд не считает нарушением тайны ознакомление с фактом или содержанием переписки (переговоров) при наличии согласия хотя бы одного из лиц, участвовавших в общении. Однако если после ознакомления с информацией были распространены без согласия сведения о частной жизни гражданина, личная или семейная тайна, то действия виновного лица подпадают под ст. 137 УК (нарушение неприкосновенности частной жизни).

Верховный суд России разъяснил, что является вмешательством в тайну личной жизни.

Вмешательство в личную жизнь становится преступлением, если речь идет о сведениях, которые гражданин сам не хотел предавать огласке (ст. 137, 138, 138.1, 139, 144.1, 145, 145.1 УК РФ).

Не может повлечь уголовную ответственность сбор или распространение таких сведений в государственных, общественных или иных публичных интересах, а также в случаях, если сведения

о частной жизни гражданина ранее стали общедоступными либо были преданы огласке самим гражданином или по его воле.

Под сбором сведений о частной жизни лица, пояснил Верховный суд, «понимаются умышленные действия, состоящие в получении этих сведений любым способом, например путем личного наблюдения, прослушивания, опроса других лиц, в том числе с фиксированием информации аудио-, видео-, фотосредствами, копирования документированных сведений, а также путем похищения или иного их приобретения».

5.7. Коммерческая тайна

Федеральный закон «О коммерческой тайне» от 29.07.2004 № 98-ФЗ регулирует отношения, связанные с установлением, изменением и прекращением режима коммерческой тайны в отношении информации, которая имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам.

5.7.1. Общие положения

Положения закона распространяются на информацию, составляющую коммерческую тайну, независимо от вида носителя, на котором она зафиксирована.

Положения закона не распространяются на сведения, отнесенные в установленном порядке к государственной тайне, в отношении которой применяются положения законодательства Российской Федерации о государственной тайне.

Коммерческая тайна – режим конфиденциальности информации, позволяющий ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду (рис. 5.9).

Информация, составляющая коммерческую тайну, – сведения любого характера (производственные, технические, экономические, организационные и другие), в том числе о результатах интеллектуальной деятельности в научно-технической сфере,

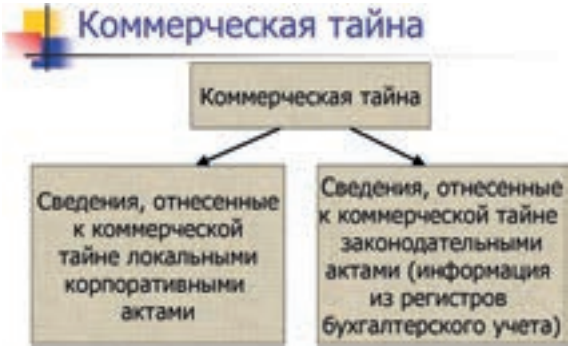

Рис. 5.9. Коммерческая тайна

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 (рис. 5.10).

Право на отнесение информации к информации, составляющей коммерческую тайну, и на определение перечня и состава такой информации принадлежит обладателю такой информации с учетом положений настоящего Федерального закона.

Информация, составляющая коммерческую тайну, полученная от ее обладателя на основании договора или 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.

Рис. 5.10. Информация, составляющая коммерческую тайну

Режим коммерческой тайны не может быть установлен лицами, осуществляющими предпринимательскую деятельность, в отношении следующих сведений:

1) содержащихся в учредительных документах юридического лица, документах, подтверждающих факт внесения записей о юридических лицах и об индивидуальных предпринимателях в соответствующие государственные реестры;

2) содержащихся в документах, дающих право на осуществление предпринимательской деятельности;

3) о составе имущества государственного или муниципального унитарного предприятия, государственного учреждения и об использовании ими средств соответствующих бюджетов;

4) 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;

5) о численности, о составе работников, о системе оплаты труда, об условиях труда, в том числе об охране труда, о показателях производственного травматизма и профессиональной заболеваемости, и о наличии свободных рабочих мест;

6) о задолженности работодателей по выплате заработной платы и социальным выплатам;

7) о нарушениях законодательства Российской Федерации и фактах привлечения к ответственности за совершение этих нарушений;

8) об условиях конкурсов или аукционов по приватизации объектов государственной или муниципальной собственности;

9) о размерах и структуре доходов некоммерческих организаций, о размерах и составе их имущества, об их расходах, о численности и об оплате труда их работников, об использовании безвозмездного труда граждан в деятельности некоммерческой организации;

10) о перечне лиц, имеющих право действовать без доверенности от имени юридического лица;

11) обязательность раскрытия которых или недопустимость ограничения доступа к которым установлена иными федеральными законами.

Обладатель информации, составляющей коммерческую тайну, по мотивированному требованию органа государственной власти, иного государственного органа, органа местного самоуправления предоставляет им 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.

На документах, 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).

5.7.2. Права и обязанности обладателя информации, составляющей коммерческую тайну

Права и обязанности обладателя информации, составляющей коммерческую тайну, возникают с момента установления им в отношении этой информации режима коммерческой тайны.

Обладатель информации, составляющей коммерческую тайну, имеет право:

1) устанавливать, изменять, отменять в письменной форме режим коммерческой тайны в соответствии с настоящим Федеральным законом и гражданско-правовым договором;

2) использовать информацию, составляющую коммерческую тайну, для собственных нужд в порядке, не противоречащем законодательству Российской Федерации;

3) разрешать или запрещать доступ к информации, составляющей коммерческую тайну, определять порядок и условия доступа к этой информации;

4) требовать от юридических лиц, 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;

5) требовать от лиц, получивших доступ к информации, составляющей коммерческую тайну, в результате действий, совершенных случайно или по ошибке, охраны конфиденциальности этой информации;

6) 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.

Меры по охране конфиденциальности информации, принимаемые ее обладателем, должны включать в себя:

1) определение перечня информации, составляющей коммерческую тайну;

2) ограничение доступа к информации, составляющей коммерческую тайну, путем установления порядка обращения с этой информацией и контроля за соблюдением такого порядка;

3) учет лиц, получивших доступ к информации, составляющей коммерческую тайну, и (или) лиц, которым такая информация была предоставлена или передана;

4) регулирование отношений по использованию информации, составляющей коммерческую тайну, работниками на основании трудовых договоров и контрагентами на основании гражданско-правовых договоров;

5) нанесение на материальные носители, содержащие информацию, составляющую коммерческую тайну, или включение в состав реквизитов документов, содержащих такую информацию, грифа «Коммерческая тайна» с указанием обладателя такой информации (для юридических лиц – полное наименование и место нахождения, для индивидуальных предпринимателей – фамилия,

имя, отчество гражданина, являющегося индивидуальным предпринимателем, и место жительства).

Меры по охране конфиденциальности информации признаются разумно достаточными, если:

1) *исключается* доступ к информации, составляющей коммерческую тайну, любых лиц без согласия ее обладателя;

2) 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.

5.7.3. Охрана конфиденциальности информации, составляющей коммерческую тайну, в рамках трудовых отношений

В целях охраны конфиденциальности информации, составляющей коммерческую тайну, работодатель обязан:

1) ознакомить под расписку работника, доступ которого к этой информации, обладателями которой являются работодатель и его контрагенты, необходим для исполнения данным работником своих трудовых обязанностей, с перечнем информации, составляющей коммерческую тайну;

2) ознакомить под расписку работника с установленным работодателем режимом коммерческой тайны и с мерами ответственности за его нарушение;

3) 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, составляющей коммерческую тайну, работник обязан:

1) выполнять установленный работодателем режим коммерческой тайны;

2) не разглашать эту информацию, обладателями которой являются работодатель и его контрагенты, и без их согласия не использовать эту информацию в личных целях в течение всего срока действия режима коммерческой тайны, в том числе после прекращения действия трудового договора;

3) возместить причиненные работодателю убытки, если работник виновен в разглашении информации, составляющей коммерческую тайну и ставшей ему известной в связи с исполнением им трудовых обязанностей;

4) передать работодателю при прекращении или расторжении трудового договора материальные носители информации, имеющиеся в пользовании работника и содержащие информацию, составляющую коммерческую тайну.

Работодатель вправе потребовать возмещения убытков, причиненных ему разглашением информации, составляющей коммерческую тайну, от лица, получившего доступ к этой информации в связи с исполнением трудовых обязанностей, но прекратившего трудовые отношения с работодателем, если эта информация разглашена в течение срока действия режима коммерческой тайны.

Причиненные работником или прекратившим трудовые отношения с работодателем лицом убытки не возмещаются, если разглашение информации, составляющей коммерческую тайну, произошло вследствие несоблюдения работодателем мер по обеспечению режима коммерческой тайны, действий третьих лиц или непреодолимой силы.

Трудовым договором с руководителем организации должны предусматриваться его обязанности по обеспечению охраны конфиденциальности составляющей коммерческую тайну информации, обладателем которой являются организация и ее контрагенты, и ответственность за обеспечение охраны конфиденциальности этой информации.

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 трудовых обязанностей.

5.7.4. Ответственность за нарушение Федерального закона «О коммерческой тайне»

1. Нарушение Федерального закона «О коммерческой тайне» влечет за собой дисциплинарную, гражданско-правовую, административную или уголовную ответственность в соответствии с законодательством Российской Федерации.

2. 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.

3. 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.

4. 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 настоящим Федеральным законом быть привлечено к ответственности.

5. По требованию обладателя информации, составляющей коммерческую тайну, лицо, указанное в предыдущем пункте,

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.

Контрольные вопросы

1. Что такое информационная безопасность?
2. Что относится к сведениям конфиденциального характера?
3. Что определяет закон Российской Федерации Об информации, информационных технологиях и о защите информации от 27 июля 2006 г. № 149-ФЗ.
4. На каких принципах основывается правовое регулирование отношений, возникающих в сфере информации, информационных технологий и защиты информации?
5. Какие права и обязанности у обладателя информации конфиденциального характера?
6. К каким информационным ресурсам не может быть ограничен доступ?
7. Какие сведения относят к персональным данным?
8. Каковы принципы обработки персональных данных?
9. Какие должны быть созданы условия для обработки персональных данных?
10. Что относится к общедоступным источникам персональных данных?
11. Что представляет собой согласие субъекта персональных данных на обработку его персональных данных?
12. Что относят к специальным категориям персональных данных?
13. Как осуществляется обработка биометрических персональных данных?
14. Каковы основные обязанности оператора при сборе персональных данных?
15. Каковы основные меры по обеспечению безопасности персональных данных при их обработке?
16. Какая ответственность лиц за нарушение требований Федерального закона «О персональных данных»?
17. Какие данные предварительного расследования должны быть защищены?
18. Что относится к служебной информации ограниченного распространения?

19. Каков порядок обращения с документами, содержащими служебную информацию ограниченного распространения?

20. Что относится к врачебной тайне?

21. Какую информацию необходимо защищать нотариальной деятельности?

22. Что относится к адвокатской тайне?

23. Что понимается под сбором сведений о частной жизни лица?

24. Что относится к коммерческой тайне?

25. Какие сведения не могут быть отнесены к коммерческой тайне в соответствии с Законом о коммерческой тайне?

26. Каковы права и обязанности обладателя информации, составляющей коммерческую тайну?

27. Какие меры по охране конфиденциальности информации должны приниматься держателем информации, относящейся к коммерческой тайне?

28. Какие меры необходимо принять работодателем в рамках трудовых отношений в целях охраны конфиденциальности информации, составляющей коммерческую тайну?

29. Какая ответственность предусмотрена за нарушение Федерального закона «О коммерческой тайне»?

ПРИЛОЖЕНИЯ

Кто хвастает знанием тайны, тот одну половину ее уже открыл,
а другую открыть не замедлит.

Жан Поль

Приложение 1

Источники права о государственной тайне в Российской Федерации

1. Нормы Конституции Российской Федерации (ч. 4 ст. 29).

2. Закон Российской Федерации «О безопасности» (от 5.03.1992 № 2446-1 с изменениями и дополнениями от 25.12.1992 № 4235-1; от 24.12.1993 № 2288; от 25.06.2002 № 116-ФЗ; от 7.03.2005 № 15-ФЗ).

3. Закон Российской Федерации «О государственной тайне» (от 21.06.1993 № 5485-1 с изменениями и дополнениями от 6.10.1997 № 131-ФЗ; от 30.06.2003 № 86-ФЗ; от 11.11.2003 № 153-ФЗ; от 29.06.2004 № 58-ФЗ; от 22.08.2004 № 122-ФЗ).

4. Отдельные нормы законов Российской Федерации:

Основы законодательства Российской Федерации об Архивном фонде Российской Федерации и архивах (ст. 7, 20, 24);

Уголовный кодекс Российской Федерации (ст. 275, 276, 283, 284);

Уголовно-процессуальный кодекс РФ (ст. 49, 183, 217, 241,328);

Гражданский процессуальный кодекс РФ (ст. 10, 26, 254);

Арбитражный процессуальный кодекс РФ (ст. 9, 11);

Кодекс Российской Федерации об административных правонарушениях (п. 3, 4 ст. 13.12, п. 2 ст. 13.13, ст. 13.14, ст. 23.45);

Таможенный кодекс Российской Федерации (ст. 10);

Налоговый кодекс Российской Федерации (ст. 165);

Градостроительный кодекс Российской Федерации (ст. 18, 54, 63);

Бюджетный кодекс Российской Федерации (ст. 195);

Трудовой кодекс РФ (ст. 37, 57, 81, 358);

Федеральный конституционный закон «О Правительстве Российской Федерации» (ст. 23);

Федеральный закон «О федеральной фельдъегерской связи» (ст. 4, 7);

Федеральный закон «Об информации, информационных технологиях о защите информации» (ст. 3, 5, 6, 9, 11, 14, 16);

Федеральный закон «О федеральной службе безопасности» (ст. 2,17, ст. 7, 9, 11, 12, 13, 17, 19, 20, 24);

Федеральный закон «Об оперативно-разыскной деятельности» ст. 12,17);

Федеральный закон «О внешней разведке» (ст. 6, 8, 9, 11, 13, 14, 18, 9, 24, 25);

Федеральный закон «О государственной охране» (ст. 14, 15, 17, 30, 32);

Федеральный закон «О порядке выезда из Российской Федерации и съезда в Российскую Федерацию» (ст. 15, 17, 37);

Федеральный закон «Об оружии» (ст. 12, 31);

Федеральный закон «Об использовании атомной энергии» (ст. 6, 19, 21, 22);

Федеральный закон «О службе в учреждениях и органах уголовно-дополнительной системы Министерства юстиции Российской Федерации» (ст. 10);

Федеральный закон «Об уничтожении химического оружия» (ст. 7);

Федеральный закон «О конкурсах на размещение заказов на поставки товаров, выполнение работ, оказание услуг для государственных нужд» (ст. 8, 12);

Федеральный закон «О государственной судебно-экспертной деятельности в Российской Федерации» (ст. 14, 16, 39);

Федеральный закон «Об официальном статистическом учете Российской Федерации» (ст. 12, 14, 15);

Федеральный закон «О статусе члена Совета Федерации и статусе депутата Государственной Думы Федерального Собрания РФ» (ст. 17);

Федеральный закон «Об основах статуса выборного лица местного самоуправления в Российской Федерации» (ст. 12);

Федеральный закон «О защите прав юридических лиц и индивидуальных предпринимателей при проведении государственного контроля (надзора)» (ст. 1);

Федеральный закон «Об аудиторской деятельности» (ст. 7);

Федеральный закон «Об адвокатской деятельности и адвокатуре в Российской Федерации» (ст. 1, 2, 6);

Федеральный закон «О несостоятельности (банкротстве)» (ст. 20);

Федеральный закон «О техническом регулировании» (ст. 5);

Федеральный закон «Об основах государственного регулирования внешнеторговой деятельности» (ст. 6, 13, 17);

Патентный закон Российской Федерации (ст. 3, 23, 30.2–30.6, 35);

Закон РФ «О правовой охране топологий интегральных микросхем» (ст. 9).

5. Подзаконные нормативные правовые акты.

5.1. Указы и распоряжения Президента Российской Федерации:

«Об утверждении перечня сведений, отнесенных к государственной тайне» (Указ Президента Российской Федерации от 30.11.1995 № 1203 с изменениями и дополнениями от 24.01.1998 № 61; от 6.06.2001 № 659; от 10.09.2001 № 1114; от 29.05.2002 № 518; от 3.03.2005 № 243 и от 11.02.2006 № 90);

«Об утверждении перечня должностных лиц органов государственной власти, наделяемых полномочиями по отнесению сведений к государственной тайне» (Распоряжение Президента Российской Федерации от 16.04.2005 № 151-рп);

«Вопросы Федеральной службы безопасности Российской Федерации» (Указ Президента Российской Федерации от 11.08.2003 № 960);

«Вопросы Федеральной службы по техническому и экспортному контролю» (Указ Президента Российской Федерации от 16.08.2004 № 1085 с изменениями и дополнениями от 22.03.2005 № 330);

«Вопросы Межведомственной комиссии по защите государственной тайны» (Указ Президента Российской Федерации от 6.11.2004 № 1286);

«О контроле за экспортом из РФ товаров и технологий двойного назначения» (Указ Президента Российской Федерации от 26.08.1996 № 1268 с изменениями и дополнениями от 4.01.1999 № 6);

«Об утверждении Положения об органах безопасности в войсках» (от 7 февраля 2000 г. № 318);

«Вопросы Службы специальной связи и информации при Федеральной службе охраны Российской Федерации» (Указ Президента Российской Федерации от 14.07.2003 № 774);

5.2. Постановления Правительства Российской Федерации:

«О предоставлении социальных гарантий гражданам, допущенным к государственной тайне на постоянной основе, и сотрудникам структурных подразделений по защите государственной тайны» (от 18.09.2006 № 573);

«Об установлении порядка рассекречивания и продления сроков засекречивания архивных документов Правительства СССР» (от 2002.1995 № 170);

«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» (от 15.04.1995 № 333 с изм. от 23.04.1996 № 509, от 30.04.1997 № 513, от 29.07.1998 № 854, от 3.10.2002 № 731 и от 17.12.2004 № 807),

«О сертификации средств защиты информации» (от 26.06.1995 № 608 с изменениями и дополнениями от 17.12.2004 № 808);

«Об утверждении Положения о военных представителях МО РФ» (от 11.09.1995 № 804);

«Об утверждении правил отнесения сведений, составляющих государственную тайну, к различным степеням секретности» (от 4.09.1995 № 870);

«Об утверждении Инструкции о порядке допуска должностных лиц и граждан Российской Федерации к государственной тайне» (от 28.10.1995 № 1050 с изменениями от 15.11.2004 № 637);

«Об утверждении Положения о Межведомственной комиссии по защите государственной тайны» (от 20.01.1996 № 71);

«Об утверждении Инструкции о порядке передачи сведений о координатах геодезических пунктов и географических объектов территории РФ иностранным государствам и международным организациям» (от 8.02.1996 № 120);

«Об утверждении Положения о порядке предоставления Российской Федерацией информации о поставках обычных вооружений» (от 3.08.1996 № 923);

«Об утверждении Положения о подготовке к передаче сведений, составляющих государственную тайну, другим государствам» (от 2.08.1997 № 973);

«Об утверждении Положения об обеспечении особого режима в закрытом административно-территориальном образовании, на территории которого расположены объекты МО РФ» (от 26.06.1998 № 655);

«Об утверждении Положения о порядке допуска лиц, имеющих двойное гражданство, лиц без гражданства, а также лиц из числа иностранных граждан, эмигрантов и реэмигрантов к государственной тайне» (от 22.08.1998 № 1003);

«Об утверждении Положения о посещении объектов по хранению химического оружия и объектов по уничтожению химического оружия (от 8.02.1999 № 143);

«Об утверждении положения о Комиссии Правительства Российской Федерации по военно-промышленным вопросам» (от 3.12.2004 № 733);

«Об утверждении Перечня территорий Российской Федерации с регламентированным посещением для иностранных граждан» (с изменениями и дополнениями от 17.11.1994 № 1273; от 27.11.1995 № 1171; от 27.12.1997 № 1641; от 2.02.2000 № 95, от 30.10.2001 № 755; от 29.04.2002 № 277; от 9.07.2002 № 513; от 11.06.2004 № 276).

6. Судебная практика:

– Постановление Конституционного Суда Российской Федерации от 27.03.1996 № 8-П;

– Определение Конституционного Суда Российской Федерации от 10.11.2002 № 293-0;

– Определение Конституционного Суда Российской Федерации от 10.11.2002 № 314-0.

Приложение 2

Основные нормативно-правовые акты в области защиты государственной тайны

1. Конституция РФ.
2. Федеральный закон РФ «О безопасности» от 28.12.2010 № 390-ФЗ.
3. Закон РФ «О государственной тайне» от 21.07.1993 № 5485-1.
4. Федеральный закон РФ «О порядке выезда из РФ и въезда в РФ» от 15.08.1996 № 114-ФЗ.
5. Федеральный закон РФ «О военно-техническом сотрудничестве Российской Федерации с иностранными государствами» от 19.07.1998 № 114-ФЗ.
6. Федеральный закон РФ «О техническом регулировании» от 27.12.2002 № 184-ФЗ.
7. Федеральный закон РФ «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ.
8. Уголовный кодекс РФ от 13.06.1996 № 63-ФЗ Кодекс РФ об административных правонарушениях от 30 12 2001 № 195-ФЗ.
9. Указ Президента РФ «Об утверждении перечня сведений, отнесенных к государственной тайне» от 30.11.1995 № 1203.
10. Указ Президента РФ «Вопросы Межведомственной комиссии по защите государственной тайны» от 06.10.2004 № 1286.
11. Указ Президента РФ «Вопросы Федеральной службы безопасности РФ» от 11.08.2003 № 960.
12. Указ Президента РФ «Вопросы Федеральной службы по техническому и экспертному контролю» от 16.08.2004 № 1085.
13. Указ Президента РФ «Вопросы военно-технического сотрудничества РФ с иностранными государствами» от 10.09.2005 № 1062.
14. Указ Президента РФ «О мерах по обеспечению информационной безопасности РФ при использовании информационно-телекоммуникационных сетей международного информационного обмена» от 17.03.2008 № 351.
15. Распоряжение «О перечне должностных лиц органов государственной власти и организаций, наделяемых полномочиями по отнесению сведений к государственной тайне» от 16.04.2005 № 151-рп.
16. Постановление Правительства РФ «Об утверждении инструкции о порядке допуска должностных лиц и граждан РФ к государственной тайне» от 06.02.2010 № 63.
17. Указ Президента РФ «О некоторых мерах государственного регулирования размещения и использования иностранных технических

средств наблюдения и контроля в ходе реализации международных договоров РФ и иных программ и проектов на территории РФ, на континентальном шельфе и в исключительной экономической зоне РФ» от 23.04.2001 № 458.

18. Постановление Правительства РФ «Об утверждении правил отнесения сведений, составляющих государственную тайну, к различным степеням секретности» от 04.09.1995 № 870.

19. Постановление Правительства РФ «Об утверждении Правил разработки перечня сведений, отнесенных к государственной тайне» от 23 июля 2005 г. № 443.

20. Постановление Правительства РФ «Об утверждении положения о порядке допуска лиц, имеющих двойное гражданство, лиц без гражданства, а также лиц из числа иностранных граждан, эмигрантов и реэмигрантов к государственной тайне» от 22.08.1998 № 1003.

21. Постановление Правительства РФ «Об утверждении перечня объектов и организаций, в которые иностранные граждане не имеют права быть принятыми на работу» от 11.10.2002 № 755.

22. Приказ «Об утверждении перечня медицинских противопоказаний для работы с использованием сведений, составляющих государственную тайну, порядка получения и формы справки об отсутствии медицинских противопоказаний для работы с использованием сведений, составляющих государственную тайну» от 26.08.2011 № 989н.

23. Постановление Правительства РФ «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» от 15.04.1995 № 333.

24. Постановление Правительства РФ «О льготном порядке лицензирования деятельности предприятий, учреждений и организаций, имеющих мобилизационные задания, осуществляющие хранение материальных ценностей государственного и мобилизационного резерва, связанной с использованием сведений, составляющих государственную тайну» от 05.04.1997 № 396.

25. Постановление Правительства РФ «Об установлении запрета на допуск программного обеспечения, происходящего из иностранных государств, для целей осуществления закупок для обеспечения государственных и муниципальных нужд» от 16.11.2015 № 1236.

26. Приказ директора ФСБ РФ об утверждении инструкции о порядке проведения специальных экспертиз по допуску предприятий,

учреждений и организаций к проведению работ, связанных с использованием сведений, составляющих государственную тайну от 23.08.1995 № 28.

27. Инструкция «О порядке проведения специальных экспертиз по допуску предприятий, учреждений и организаций к проведению работ, связанных с использованием сведений, составляющих государственную тайну» от 23.08.1995 №28.

28. Постановление Правительства РФ «Об утверждении положения о подготовке и передаче сведений, составляющих государственную тайну, другим государствам или международным организациям» от 02.08.1997 № 973.

29. Постановление Правительства РФ «Об утверждении инструкции о порядке передачи сведений о координатах геодезических пунктов и географических объектов территории РФ иностранным государствам и международным организациям» от 08.02.1996 № 120.

30. Постановление Правительства РФ «Об утверждении правил выполнения геодезических и картографических работ на отдельных территориях РФ и о признании утратившими силу некоторых постановлений правительства РФ» от 09.02.2017 № 159.

31. Постановление Правительства РФ «О порядке проведения проверки наличия в заявках на выдачу патента на изобретение или полезную модель, созданные в РФ, сведений, составляющих государственную тайну» от 24.12.2007 № 928.

32. Постановление Правительства РФ «Об утверждении правил организации и осуществления федерального государственного контроля за обеспечением защиты государственной тайны» от 22.11.2012 № 1205.

33. Постановление Правительства РФ «О государственной системе защиты информации в РФ от иностранных технических разведок и от ее утечки по техническим каналам» от 15.09.1993 № 912- 51.

34. Постановление Правительства РФ «О сертификации средств защиты информации» от 26.06.1995 № 608.

35. Постановление Правительства РФ «Об особенностях оценки соответствия продукции (работ, услуг), используемой в целях защиты сведений, составляющих государственную тайну или относимых к охраняемой в соответствии с законодательством РФ иной информации ограниченного доступа, и продукции (работ, услуг), сведения о которой составляют государственную тайну, предназначенной для эксплуатации в загранучреждениях РФ, а также процессов ее проектирования (включая изыскания), производства, строительства, монтажа, наладки, эксплуатации, хранения, перевозки, реализации, утилизации и захоронения, об особенностях аккредитации органов по сертификации и испытательных

лабораторий Центров, выполняющих работы по подтверждению соответствия указанной продукции (работ, услуг), и о внесении изменения в Положение о сертификации средств защиты информации» от 21.04.2010 № 266.

36. Приказ Министерства здравоохранения и социального развития «О порядке выплаты ежемесячных процентных надбавок гражданам, допущенным к **государственной тайне** на постоянной основе, и сотрудникам структурных подразделений по защите **государственной тайны»** от 19.05.2011 № 408н.

37. Постановление Правительства РФ «Об организации повышения квалификации специалистов по защите информации и должностных лиц, ответственных за организацию защиты информации в органах государственной власти, органах местного самоуправления, организациях с государственным участием и организациях оборонно-промышленного комплекса» от 06 05 2016 № 399.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. «Конституция Российской Федерации» (принята всенародным голосованием 12.12.1993) (с учетом поправок, внесенных Законами РФ о поправках к Конституции РФ от 30.12.2008 № 6-ФКЗ, от 30.12.2008 № 7-ФКЗ, от 05.02.2014 № 2-ФКЗ, от 21.07.2014 № 11-ФКЗ).

2. Закон РФ от 21.07.1993 № 5485-1 «О государственной тайне».

3. Постановление Правительства РФ от 06.02.2010 № 63 «Об утверждении Инструкции о порядке допуска должностных лиц и граждан Российской Федерации к государственной тайне».

4. Указ Президента РФ от 30.11.1995 № 1203 «Об утверждении Перечня сведений, отнесенных к государственной тайне».

5. Постановление Правительства РФ от 06.02.2010 № 63 (ред. от 19.04.2019) «Об утверждении Инструкции о порядке допуска должностных лиц и граждан Российской Федерации к государственной тайне».

6. Постановление Правительства РФ от 23.08.2018 № 984 «Об утверждении Правил подтверждения степени секретности сведений, с которыми предприятия, учреждения и организации предполагают проводить работы, связанные с использованием сведений, составляющих государственную тайну, и о внесении изменения в п. 5 Положения 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».

7. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ.

8. Федеральный закон «О персональных данных» от 27.07.2006 № 152-ФЗ.

9. Федеральный закон от 03.07.2016 № 226-ФЗ «О войсках национальной гвардии Российской Федерации».

10. Федеральный закон «О связи» от 07.07.2003 № 126-ФЗ.

11. Гражданский кодекс Российской Федерации (ГК РФ) от 30 ноября 1994 г. № 51-ФЗ.

12. Кодекс Российской Федерации об административных правонарушениях» от 30.12.2001 № 195-ФЗ (с изм. и доп. от 12.04.2020).

13. «Трудовой кодекс Российской Федерации» от 30.12.2001 № 197-ФЗ.

14. «Уголовный кодекс Российской Федерации» от 13.06.1996 № 63-ФЗ (с изм. и доп. от 12.04.2020).

15. **Бакаева О. Ю.** Государственный контроль в сфере защиты государственной тайны: актуальные вопросы правового регулирования / О. Ю. Бакаева // Информационная безопасность регионов. – 2013. – № 1 (12). – С. 93–97.

16. **Аленов А.** Концерн шпионажа и диверсий / А. Аленов, В. Андреев. – М. : Молодая Гвардия, 2016. – 334 с.

17. **Бержье Ж.** Промышленный шпионаж / Ж. Бержье. – М. : Международные отношения, 2011. – 176 с.

18. **Вильям Ч.** Любовь и шпионаж. Два дня и три ночи / Чарльз Вильям, Алистер Маклин. – М. : Российское право, 2011. – 448 с.

19. **Дамаскин И. Б.** Разведки и шпионаж / И. Б. Дамаскин. – М. : Вече, 2017. – 422 с.

20. Оружие шпионажа. 1993–1994 : каталог-справочник. – М. : Империал, 2016. – 240 с.

21. Государственная тайна и ее защита в Российской Федерации : учеб. пособие / под ред. М. А. Вуса и А. В. Федорова. – СПб. : Юридический центр Пресс, 2007. – 752 с.

22. Постановление Правительства РФ от 3 ноября 1994 г. № 1233 «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти, уполномоченном органе управления использованием атомной энергии и уполномоченном органе по космической деятельности» (с изменениями и дополнениями).

Глухов Владимир Викторович
Зайцев Анатолий Иннокентьевич
Братушка Андрей Николаевич

ЗАЩИТА ГОСУДАРСТВЕННОЙ ТАЙНЫ В РОССИЙСКОЙ ФЕДЕРАЦИИ: ПОНЯТИЯ, ОРГАНИЗАЦИЯ, ПРАВИЛА, ОТВЕТСТВЕННОСТЬ

Учебное пособие

Корректор *Н. Б. Цветкова*
Компьютерная верстка *Е. Н. Никулкиной*, *Е. Г. Орловского*
Дизайн обложки *О. А. Костюшенко*

Налоговая льгота – Общероссийский классификатор продукции
ОК 005-93, т. 2; 95 3005 – учебная литература

Подписано в печать 03.09.2020. Формат 60×84/16. Печать цифровая.
Усл. печ. л. 15,0. Тираж 120. Заказ 1305.

Отпечатано в Издательско-полиграфическом центре
Политехнического университета.
195251, Санкт-Петербург, Политехническая ул., 29.
Тел.: (812) 552-77-17; 550-40-14.