МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

САНКТ-ПЕТЕРБУРГСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИНФОРМАЦИОННЫХ ТЕХНООГИЙ, МЕХАНИКИ И ОПТИКИ

Жигулин Г.П.

ОРГАНИЗАЦИОННОЕ И ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Санкт-Петербург

2014

Жигулин Г.П. Организационное и правовое обеспечение информационной безопасности, – СПб: СПбНИУИТМО, 2014. – 173с.

В учебном пособии, на основе анализа существующей нормативно-правовой базы, изложены вопросы организационно-правовой оценки защиты информации в органах государственной власти, на предприятиях и в организациях различных форм собственности, коммерческих организациях и учреждениях. Рассмотрены понятия конфиденциальности информации, принципы и критерии отнесения информации к коммерческой тайне, вопросы организации допуска и доступа персонала к конфиденциальной информации, основные направления и методы работы по организации допуска к конфиденциальной информации, также рассмотрены вопросы аналитической работы и контроля состояния защиты конфиденциальной информации.

Рецензенты: дтн, профессор В.А.Сарычев
дтн, профессор Ю.М.Русаков
дтн, снс, В.Г.Швед

Рекомендовано Ученым советом Института комплексного военного образования СПб НИУ ИТМО протокол № 1 от 13.01.2014 г. в качестве учебного пособия для бакалавров, магистрантов и аспирантов, обучающихся по направлению подготовки «Информационная безопасность», которые по роду образования и деятельности погружены в проблематику нормативно-правовой оценки защиты информации.

В 2009 году, Университет стал победителем многоэтапного конкурса в результате которого определены двенадцать ведущих Университетов России, которым присвоена категория «Национальный исследовательский университет». Министерством образования и науки Российской Федерации была утверждена программ его развития на 2009-2018 годы. В 2011 году Университет получил наименование «Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики».

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

В настоящее время при решении задач защиты конфиденциальной информации в органе государственной власти, на предприятии, в коммерческой организации или в учреждении[1] наиболее значимую роль играют меры организационного характера, способные по своей сути объединить в комплексе все имеющиеся способы и методы защиты информации на основе действующих норм и правил.

Это обусловлено, прежде всего, вполне объяснимым стремлением руководителей организаций и предприятий создать и на необходимом уровне поддерживать эффективную систему защиты информации, способную в каждом конкретном случае с учетом специфики деятельности предприятия определить необходимую совокупность сил и средств, а также мероприятий, используемых при решении задач по защите информации.

Организаторские функции руководителей предприятия играют важную роль в достижении основных целей его деятельности. Не случайно выбор управленческих решений не может быть эффективным без строгой системы применения нормативно-методических документов на основе опыта работы предприятия в той или иной области, в нашем случае, - области, связанной с защитой конфиденциальной информации.

Многообразие функций и задач, решаемых предприятиями различных сфер деятельности и организационно-правовых форм, требует постоянного совершенствования системы защиты конфиденциальной информации, принятия новых нормативных актов, методических документов, инструкций и руководств для работников предприятия.

Объединить в себе всю имеющуюся информацию по вопросам защиты конфиденциальной информации, четко определить направления ее защиты и расставить в нужный момент приоритеты в использовании необходимых сил и средств, способов и методов ее защиты - приоритетная задача организационной составляющей системы защиты конфиденциальной информации.

Для решения данной задачи необходимы разносторонние знания нормативно-правовых основ защиты информации, направлений деятельности предприятий, очередности и порядка принятия управленческих решений в зависимости от выбранного комплекса мероприятий.

В данной монографии раскрываются организационные и правовые основы защиты конфиденциальной информации, основные принципы, силы, средства, условия, а также направления деятельности руководителей предприятия по организации защиты конфиденциальной информации, а также дается краткая история возникновения органов защиты информации.

[1] В дальнейшем в тексте данного учебного пособия органы государственной власти, предприятия, коммерческие организации и учреждения для краткости будут именоваться предприятиями, если иное не оговорено особо.

1. ИСТОРИЯ ВОЗНИКНОВЕНИЯ ОРГАНОВ ЗАЩИТЫ ИНФОРМАЦИИ

Шпионаж существовал всегда, по крайней мере, со времен Прометея, который осуществил несанкционированную другими богами передачу людям совершенно секретной технологии получения огня, что впоследствии привело к космическим полетам. Человек всегда стремился знать как можно больше о соседях. В нашу постиндустриальную эру информация приобрела решающую роль.

В большинстве индустриально развитых стран информация является первоосновой всех аспектов развития общества. Преимущество и специфика информации заключается в том, что она не исчезает при потреблении, не передается полностью при обмене (оставаясь в информационной системе и у пользователя), является "неделимой", т.е. имеет смысл только при достаточно полном наборе сведений, что качество ее повышается с добавлением новой информации. В настоящее время предприятий, занимающиеся несанкционированным получением информации, с целью извлечения прибыли, становиться все больше и больше.

За всю историю своего существования человечество в этой области накопило значительный опыт.

Самыми ранними источниками получения сведений в эпоху, когда человек верил во вмешательство в его дела сверхъестественных сил, были пророки, провидцы, оракулы, прорицатели и астрологи.

К 400 году до н. э. Восток значительно опередил Запад в искусстве разведки. Сунь Цзы писал: "То, что называют предвидением, не может быть получено ни от духов, ни от богов, ни посредством расчетов. Оно должно быть добыто от людей, знакомых с положением противника"[2].

Преуспели в шпионаже многие государи и частные лица. Прекрасно поставленная служба разведки помогала купцам Венеции и банкирскому дому Фуггеров, фирме Круппа и дому Ротшильдов. Методы практически не менялись столетиями: подкупали, шантажировали, посылали послов-шпионов, перехватывали письма, читали пергаменты в библиотеках и монастырях. Когда удавалось, подсматривали и подслушивали. Одновременно со шпионажем возникла и необходимость в защите информации. Методы защиты информации являлись адекватными возникающим угрозам: выставлялась надежная охрана, лицам, работающим с конфиденциальной информацией, платилось очень хорошее жалование, информация шифровалась.

Криптография возникла с появлением письменности и явилась, чуть ли не самым надежным способом защиты информации. Методы секретной переписки были изобретены независимо в различных государствах древнего Востока, таких как Египет, Китай и Шумер. (На раскопках было найдено множество глиняных табличек с клинописными знаками, записанными в несколько слоев, первоначальная запись замазывалась глиной и поверх нее наносилась новая). Наибольшее развитие криптография получает в полисах Древней Греции, а позже в Риме, где было изобретено множество известных шифров.

Все вышеуказанные способы защиты информации применялись и в Древней Руси. Необходимо отметить роль Ивана IV (Грозного) в совершенствовании

[2] Роуан Р. Очерки секретной службы. Из истории разведки, СПб, 1992.

системы защиты государственной тайны путем создания "Тайного приказа", на который возлагались функции защиты информации.

В России необходимость создания выделенной криптографической службы была осознана на государственном уровне во времена Петра I, когда за рубежом оказалось множество дипломатических представительств, и систематическая связь с ними должна была быть доверена почте, а не эпизодически посылаемым курьерам. Так, впервые в России, в Коллегии Иностранных Дел возникла криптографическая служба.

Петр I также обращал особое внимание и на вопросы сохранения государственной тайны во всех сферах деятельности государства, так в январе 1724 года им был издан Указ: "О делах тайности подлежащих" (см. рисунок 1.1).

Позже, вопросы защиты государственной тайны и криптографии были подняты на высочайший уровень в годы царствования Екатерины II[3].

В этот период организация защиты государственной тайны России считалась лучшей в мире, так как к работе были привлечены лучшие умы государства (академики Христиан Гольдбах, Карл фон Бреверн, Франц Эпинус и др.).

До середины XIX века не существовало специальных разведывательных служб целенаправленно занимавшихся, на протяжении длительного периода времени, сбором и анализом информации о ситуации в других странах.

Только после Австро-Прусской войны 1866 года началось активное реформирование уже существующих спецслужб и создание новых. Это было связано с тем, что Вильгельм Штибер - руководитель разведки Пруссии, сумел обеспечить свое правительство всей необходимой информацией о политических и военных противниках (дислокация войск, их моральный дух, задачи и планы и т.п.), которой раньше Бисмарк не располагал.

Уже в первые годы 20 века все крупные мировые державы начали подготовку к войне, напряжено наблюдая за тем, что делают потенциальные союзники и противники. В мирное время немногочисленные аппараты спецслужб "охотились" за мобилизационными планами, новинками военной техники и информацией о приготовление к будущей войне.

Как следствие этого, в военном ведомстве России начались активные действия по созданию и совершенствованию системы по защите государственной тайны. Работа велась по четырём направлениям: создание и совершенствование системы контрразведывательных органов, организация комплексной системы защиты информации, содержащей военную тайну, совершенствование системы фельдъегерской связи, организация военной цензуры.

В русском обществе проблема противодействия шпионажу противника регулярно обсуждалась на страницах газет: "Русский инвалид", "Новое время", "Военный сборник". Но все материалы носили дискуссионный характер и были интересны лишь узкой группе специалистов и любопытных.

Вплоть до 1912 года работы по созданию системы защиты информации государства велись крайне медленно и непоследовательно.

---

[3] В своих воспоминаниях академик Христиан Гольдбах писал: "Императрица Екатерина II блестяще владела навыками разведывательной и контрразведывательной работы". (Новик В.К. Христиан Гольдбах и Франц Эпинус (из истории шифровальных служб России XVIII века). Доклад на конференции "Математика и безопасность информационных технологий" (МаБИТ-03, МГУ, 23-24.10.2003г.)).

УКАЗЫ

Блаженныя и вѣчнодостойныя памяти

ГОСУДАРЯ ИМПЕРАТОРА

ПЕТРА ВЕЛИКАГО

САМОДЕРЖЦА ВСЕРОССІЙСКАГО,

состоявшіеся съ 1714, по кончину Его Императорскаго Величества, Генваря по 28 число 1725 году.

Напечатаны по указу

ВСЕПРЕСВѢТЛѢЙШЕЙ ДЕРЖАВНѢЙШЕЙ ВЕЛИКОЙ

ГОСУДАРЫНИ ИМПЕРАТРИЦЫ

АННЫ ІОАННОВНЫ

САМОДЕРЖИЦЫ ВСЕРОССІЙСКОЙ.

При Императорской Академіи Наукъ въ Санктпетербургѣ
1780 года.

О дѣлахъ тайности подлежащихъ.

Генваря 17 дня.

Его Императорское Величество будучи въ зимнемъ домѣ Генваря 13 дня 1724 году указалъ о дѣлахъ, которыя тайности подлежатъ въ Государственныхъ дѣлахъ онаго опинюдъ въ партикулярныхъ письмахъ ни къ кому не писать, нижѐ къ тому, отъ кого отправленъ, кромѣ настоящихъ реляцій. А ежели какое препятствіе отъ кого въ томъ или иномъ будетъ его дѣлу, то писать вольно, куды за благо кто разсудитъ, только упоминая о врученномъ ему дѣлѣ генерально, отъ чего оному поврежденїе есть; также ежели случатся дѣла постороннія тайнѣ подлежащія, а въ реляціяхъ къ тому, отъ кого отправленъ, писать будетъ за какимъ подозрѣнїемъ не возможно, то вольно писать, кому въ томъ повѣритъ, а о врученномъ своемъ никакъ инакъ, только какъ выше писано, подъ жестокимъ наказаніемъ по винѣ преступленія. И сей указъ всякому писать въ инструкціяхъ.

Подлинной за подписаніемъ Правительствующаго Сената.

Рис. 1.1. Указ Петра I "О делах тайности подлежащих".

В 1912 году в России был принят самый прогрессивный в Европе законодательный акт[4], направленный на правовое обеспечение защиты государственной тайны и противодействие иностранному шпионажу, который значительно расширил понятие государственной измены путём шпионажа, изменив, с одной стороны, изложения некоторых статей "Уголовного уложения", а с другой стороны, ввел в действия ряд новых карательных постановлений, предусматривающих уголовную ответственность за некоторые виды шпионажа, ранее уголовно ненаказуемые.

Когда началась первая мировая война, то выяснилось, что армия и вместе с ней и государство, не способны обеспечить необходимый уровень защиты военной тайны. И только 22 июня 1914 года газета "Русский инвалид" опубликовала обращение к гражданам Российской империи. Это было первая попытка выразить мнение властей об отношение к защите военной тайны в Российской империи. В нём власти призывали население хранить в тайне информацию о дислокации, перемещение и численности войск. Население призывали не верить различным слухам и сохранять спокойствие. Правительство обещало информировать о реальной обстановке на фронте.

К сожалению, время было упущено. Волна шпиономании, захлестнувшая Россию, как и другие европейские страны, не способствовало активизации мероприятий по защите военной тайны.

Вопросами ведение секретной переписки по всем вопросам занимался восьмой стол VII отделения ведение военной статистики иностранных государств Второго Управления Генерал-Квартирмейстера. Это отделение совмещало в себе функции обычной библиотеки и спецотдела, регламентирующего вопросы допуска работы с секретными документами. Была в Генеральном штабе и своя криптографическая служба.

Все вопросы, связанные с организацией хранения, пересылки и обработки мобилизационных планов регламентировались специальной инструкцией. Способов хранения секретных документов было два: в железном ящике; в железном ящике, вложенном в деревянный сундук.

Ещё одним направлением была цензура печатных изданий. Например, до начало русско-японской войны, даже такой специальный военный орган, как, "Русский инвалид" помещал на своих страницах все распоряжения военного министерства, в том числе и секретные. А ежегодно издаваемое "Краткое описание сухопутных сил", содержало подробный перечень всех частей царской армии с указанием мест их постоянной дислокации и фамилиями командиров дивизией, полков и отдельных батальонов (стрелковых и резервных), можно купить любому желающему.

Особенно ярко это проявилось в русско-японскую войну. Все развертывания наших резервных частей, перемещение второочередных вместо полевых, ушедших на Дальний Восток печатались в "Русском Инвалиде". После каждого боя, в том же официальном печатном органе российской армии, печатались списки убитых и раненых офицеров с указанием их частей.

---

[4] Закон Российской империи от 5.07.1912 г. "Об изменении действующих законов о государственной измене путем шпионства в мирное время". (Чертопруд С. В. Законодательные акты по защите гостайны в Российской империи в начале XX века, журнал "Вопросы защиты информации", М., № 4 (35), 1996).

В Российской империи не существовало централизованной системы защиты государственной тайны. МИД, Военное ведомство и Департамент полиции самостоятельно прилагали усилия по обеспечению сохранности государственной тайны. При этом Департамент полиции славился своей системой конфиденциального делопроизводства, а МИД и Военное ведомство имели достижения в области криптографии. В то же время предпринимаемые мероприятия носили хаотичный характер и не могли обеспечить эффективной защиты государственных секретов.

Начиная с 1918 года молодой Советской республике пришлось разработать и создать эффективную систему защиты государственной тайны, которая, в модифицированном состоянии, продолжает существовать и в наши дни. Ее основные принципы и структура были сформированы в 20-30 годы. Затем, только редактировались руководящие документы и менялись названия органов защиты информации.

Первым шагом в создание централизованной системы защиты государственной тайны можно назвать организацию органов контрразведки. Была введена система паспортного контроля для упорядочения процесса въезда и выезда на территорию Советской республики. В частности, в ноябре 1917 был утверждены декретом СНК "Правила въезда и выезда из России"[5]. А 24 апреля 1919 года был издан декрет СНК "О порядке выдачи заграничных паспортов"[5]. Правда, эффективность этих мер в тот период была не высокой. Почти любой желающий мог оформить себе фальшивые или поддельные документы.

В 1920 году НКВД, согласно Постановлению Совета труда и обороны от 18 августа 1920 года, было предоставлено исключительное право определять порядок въезда и выезда в отдельные местности. Таким образом, впервые в истории России, было введено понятие территории или района с особым режим. Значительно позднее эти районы и территории трансформируются в "закрытые" города. Некоторые из них существуют и по настоящее время.

До 1921 года не предпринимались попытки упорядочить порядок обработки и хранения документов, содержащих государственную тайну. Например, в изданном Управлением Военно-учебных заведений Западного фронта в 1921 году учебном пособие "Военная тайна" рассматривались не только простейшие методы организации секретного делопроизводства, но и перечень сведений, которые могли являться военной тайной. Автор учебного пособия, бывший офицер военной разведки царской армии Н.Е. Какурин, пытался, таким образом, решить проблему с защитой военной тайны в действующей Красной армии.

Одновременно с этой книгой, 13 октября 1921 года Декретом СНК был утвержден "Перечень сведений составляющих тайну и не подлежащих распространению"[5]. Сведения делились на две группы: военного и экономического характера.

Первая попытка навести порядок в сфере обработки и хранения секретных документов была предпринята 30 августа 1922 года. Тогда Секретариат ЦК РКП(б) принял постановление "О порядке хранения и движения секретных документов"[5]. В этом документе впервые было зафиксировано, что для организации и ведения секретного делопроизводства необходимо создание секретных частей.

[5] Роуан Р. Очерки секретной службы. Из истории разведки, СПб, 1992.

В том же году Оргбюро ЦК РКП(б) приняло постановление "О порядке хранения секретных постановлений ЦК РКП(б)"[6]. Аналогичный документ был издан и в Красной Армии. Приказ РВСР № 2011 определял порядок обращения с совершенно секретной корреспонденцией.

Постановлением СНК 24 апреля 1926 года был утвержден новый открытый "Перечень сведений, являющихся по своему содержанию специально охраняемой государственной тайной"[6]. Все сведенья были разделены на три группы: сведения военного характера, сведенья экономического характера и сведенья иного характера. Кроме этого было введено три категории секретности. Согласно Перечню, указанным в нем сведеньям, был присвоен один из трех грифов секретности: совершенно секретно, секретно и не подлежит оглашению.

В 1926 году был принят набор общесоюзные инструкций, которые регламентировали отдельные вопросы организации и ведения секретного делопроизводства: "Инструкция по ведению секретного и шифровального делопроизводства", "Инструкция местным органам ОГПУ по наблюдению за постановкой секретного и мобилизационного делопроизводства", "Инструкция по ведению архивного делопроизводства и сдаче дел в органы Центрархива", "Инструкция о порядке заготовления и конвертования корреспонденции, пересылаемой дипломатической почтой", "Инструкция о порядке стенографии на секретных совещаниях и заседаниях", "Инструкция о порядке ведения и хранения секретной переписки". В 1929 году была принята: "Инструкция местным органам ОГПУ по наблюдению за состоянием секретного и мобилизационного делопроизводства учреждений и организаций"[6].

В конце 20 годов была проведена унификация состава секретных органов и установлена стандартная номенклатура должностей секретных аппаратов учреждений и организаций. Структура секретных органов предусматривала: секретное делопроизводство, машбюро, чертежное бюро, стенографическое бюро, группа контроля, группа по учетно-распределительной работе, бюро пропусков и справок. Конкретный состав секретных органов определялся наркоматами по согласованию со спецотделом при ОГПУ. Службы защиты государственной тайны назывались по-разному: секретные части, подотделы секретного делопроизводства, шифровальные отделы и т.д.

Принятые в конце 20 годов инструкции действовали до 1940 года, а номенклатура должностей, а структура режимно-секретных органов просуществовала без изменений значительно дольше.

Наиболее эффективно централизованная система защиты государственной тайны работала в 60-80 годы, хотя в тот период не предпринималось почти никаких радикальных мер по ее модификации - так эффективны и оптимальны были принципы, заложенные еще в 20 годы.

С появлением телеграфа, телефона, а позже и средств вычислительной техники, появились новые возможности получения конфиденциальных сведений. Гигантское количество информации стало перехватываться с использованием технических средств разведки, влияя на ведение войн.

Начиная с 1960 года, остро возникла необходимость в защите информации, циркулируемой в информационно-вычислительных сетях от технических средств разведки иностранных государств.

---

[6] Роуан Р. Очерки секретной службы. Из истории разведки, СПб, 1992.

Так в 1976 году в СССР появились первые органы защиты информации на объектах вычислительной техники[7].

В целях унификации всех органов по защите информации различных министерств и ведомств в 1993 году в России были определены органы защиты государственной тайны и образованы единые структурные подразделения по защите государственной тайны[8].

2. КОНЦЕПТУАЛЬНЫЕ ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В настоящее время обладание информацией становится одним из решающих факторов контроля над решением любых проблем мирового сообщества.

Информация стала фактором, способным привести к крупномасштабным авариям, военным конфликтам и поражению в них, дезорганизовать государственное управление, финансовую систему, работу научных центров. В то же время обладание информацией способствует развитию всех сфер деятельности государства в целом и отдельно взятого предприятия в частности и, в конечном счете, приводит к значительным успехам в экономике, бизнесе, финансах. Однако, обладание ценной информацией, возлагает на субъекты, имеющие на нее соответствующие права, высокую степень ответственности за ее сохранность и защиту от возможного внешнего воздействия различного рода факторов и событий, носящих как преднамеренный, так и случайный характер.

Информация и информационные технологии сегодня определяют пути и направления развития любого общества и государства, коренным образом влияют на формирование человека как личности, оказывают решающее воздействие на определение его роли и места в обществе, активизируют и мотивируют сферы его познания в науке, истории и других областях.

Программы развития информационных технологий ведущих мировых держав, их финансирование на государственном уровне выходят на первое место, опережая ракетные и космические программы. Вместе с тем, стремительность развития информационных технологий все больше отдаляет нас от понимания сущности самой информации, форм и способов ее проявления, методов воздействия информации на развитие общества, государства и личности.

Эти знания нам необходимы, прежде всего, для понимания общих принципов и основ информационной безопасности, формирования всего спектра связанных с ней проблем и определения путей их решения.

Термин "информация" происходит от латинского "information", что означает разъяснение, изложение. Однако разные науки сегодня вкладывают в это понятие различное содержание. Информация зачастую определяется через различные свойства материи, или путем выделения ее содержательного (семантического), ценностного (прагматического) аспектов.

---

[7] Органы защиты информации на объектах вычислительной техники образованы Постановлением ЦК КПСС и Совета Министров СССР от 4.12.1976 года "Об обеспечении безопасности в автоматизированных системах управления войсками и вычислительной техники общего применения от утечки информации за счет побочных электромагнитных излучений и наводок и несанкционированного доступа".

[8] Статья 20 Закона РФ от 21.07.1993 г. № 5485-1 "О государственной тайне".

Диапазон толкования термина "информация" достаточно широк: от частного, бытового представления информации (сведения, сообщения, подлежащие переработке) до философского как наиболее общего и мировоззренческого ее понимания.

Ни наука, ни человек, ни общество сегодня не могут эффективно и динамично развиваться без сбора, передачи, накопления и использования информации с целью получения новых знаний.

В связи с этим, из всего многообразия представлений о толковании термина "информация" наиболее четко выделяются две основные точки зрения на сущность информации как явления: органическая и атрибутивная.

Атрибутивная точка зрения на толкование понятия "информация" предполагает тесное увязывание информации с материей. В основе такого подхода к определению информации лежит предположение о возможности обмена информацией между объектами неживой природы. Однако практика показывает, что эта точка зрения сегодня не может в полной мере представить сущность информации, которой обмениваются с целью ее использования в интересах анализа, переработки и применения субъекты "живой" природы - организмы, а также создаваемые и управляемые ими системы и механизмы.

Таким образом, органическое представление информации в настоящее время более соответствует реальному миру и, в связи с этим, является более применяемым и используемым в повседневной жизни.

Основой органического мировоззрения на толкование понятия "информация" является свойство живой материи - организмов, отражать объективную реальность и использовать результаты этого отражения для применения в условиях быстроменяющейся обстановки и динамичного развития условий существования - самой жизни. Это мировоззрение более относится к категории философского понятия, однако позволяет понять и проанализировать сущность и информационных, и коммуникационных процессов, являющихся сегодня неотъемлемой частью и непременным условием нашего времени.

Согласно органическому подходу к толкованию понятия информации она представляет собой результаты отражения движения объектов материального мира, запечатленные в организме или коллективе организмов и используемые ими для адаптации к изменениям окружающего мира.

Человек как объект живой природы наделен способностью адаптации к изменениям окружающей действительности. В отличие от других организмов, человек способен не только приспосабливаться к реальной жизни и условиям, но и оказывать воздействие на условия своего существования. Реализация этих способностей человека целиком и полностью основывается на восприятии, накоплении и использовании информации в форме сведений, а также получении и передаче ее в форме сообщений.

Следовательно, сведения и сообщения являются основными формами проявления информации.

Сведения - запечатленные в организме результаты отражения движения объектов материального мира.

Сообщения - набор знаков, с помощью которых сведения могут быть переданы другому организму и восприняты им.

По своей сути сообщение способно порождать в организме человека определенные сведения, и, с этой точки зрения, очевидно, что оно содержит эти све-

дения. Преобразование сведений в сообщения осуществляется с использованием алгоритмов кодирования передаваемых элементов "информационной" модели в набор знаков сообщения, а сообщений - в сведения - с использованием алгоритмов декодирования поступившего набора знаков в элементы "информационной" модели человека. Без реализации упомянутых алгоритмов кодирования и декодирования сообщение представляется простым набором знаков (символов).

В этой связи нельзя не сказать о свойствах информации, представленной в форме сведений и в форме сообщений.

Основными свойствами информации в форме сведений являются:

динамичность - возможность изменения, посредством получения и обработки сведений, отношений между объектами материального мира, запечатленными в организме, а также их параметрами и характеристиками;

духовность - возможность восприятия сведений органами чувств;

субъективность - зависимость количества и ценности сведений от получающего и обрабатывающего их субъекта;

неуничтожаемость - невозможность физического уничтожения сведений.

Информация, представленная в форме сообщений, в свою очередь, характеризуется следующими свойствами:

статичность - независимость набора знаков, из которых сформировано сообщение, от времени, прошедшего с момента его создания;

материальность - способности сообщения оказывать воздействие на органы чувств;

объективность - независимость сообщения от получающего и обрабатывающего их субъекта;

уничтожаемость - возможность физического уничтожения сообщения;

ограниченная воспроизводимость - невозможность точного воспроизведения сообщения без его закрепления (копирования) на некотором материальном носителе.

Таким образом, понятие "информация" объединяет два разнородных понятия - сведения и сообщения, обладающие определенными, характеризующими их свойствами, и, как следствие, обладающие способностью являться предметами человеческой деятельности.

Современный этап развития нашего общества характеризуется возрастающей ролью информационной сферы в целом, которая представляет собой совокупность информации, информационной инфраструктуры, субъектов, осуществляющих сбор, формирование, распространение и использование информации, а также системы регулирования возникающих при этом общественных отношений. Информационная сфера, являясь самообразующим фактором жизни общества, активно влияет на состояние политической, экономической, оборонной и других составляющих безопасности Российской Федерации.

Из всех составляющих информационной сферы, в рамках рассматриваемых в настоящем учебном пособии вопросов ключевыми, наиболее выделяющимися понятиями, являются информация и информационные технологии.

При рассмотрении вопросов, связанных с применением информационных технологий, осуществлении права на поиск, получение, передачу, производство и распространение информации, а также на обеспечение ее защиты используются следующие понятия информации и информационных технологий:

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

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

В наше время информация и информационные технологии являются одними из основных, необходимых условий жизни общества и государства.

Информационные технологии в значительной степени определяют возможности человека по формированию, распространению и потреблению информации, накоплению обществом социально важных сведений. Информационные технологии обусловливают возможности общества по воссозданию приемов, моделирующих интеллектуальную деятельность человека в создаваемых им средствах производства, предметах потребления, ведении вооруженной борьбы, обеспечении социальной коммуникации.

По мере развития научно-технического прогресса, возрастания роли информационных технологий в повседневной жизни, их проникновения во все сферы деятельности общества и государства, возрастает роль информационной безопасности личности, общества и государства, а ее обеспечение занимает особое место в деятельности всех государственных институтов.

Одним из принципов правового регулирования отношений, возникающих в сфере информации, информационных технологий и защиты информации является "обеспечение безопасности Российской Федерации при создании информационных систем, их эксплуатации и защите содержащейся в них информации"[9], по иному - обеспечение информационной безопасности нашего государства.

Под ***информационной безопасностью Российской Федерации*** понимается состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства. Национальная безопасность Российской Федерации существенным образом зависит от обеспечения информационной безопасности, и в ходе технического прогресса эта зависимость будет возрастать.

Информационная инфраструктура является объектом национальных интересов в связи с ее использованием для реализации: важных функций общества и, прежде всего, обмена циркулирующей в обществе информации; управления социальными и технологическими процессами, войсками и оружием, обеспечением безопасности критически важных производств; коммерческих операций торгового и банковского характера, оказания информационных услуг. При этом безопасность информационной инфраструктуры заключается в защищенности от угроз ее способности выполнять основные социальные функции.

Национальные интересы в информационной сфере определяются, прежде всего, той ролью, которую играет информация, информационные технологии и созданная на их базе информационная инфраструктура в обеспечении устойчивого развития нации в конкретных исторических условиях, а также в сохранении национальной идентичности. Эти интересы образуются сбалансированной совокупностью социальных интересов индивида как личности, интересов общества и государства, реализуемых в информационной сфере, включая их интересы в ис-

[9] Федеральный закон РФ от 27.07.2006 г. № 149-ФЗ "Об информации, информационных технологиях и защите информации".

пользовании информационной сферы для сохранения национальной идентичности.

Социальные интересы личности заключаются в поддержании определенного правового статуса человека и гражданина в информационной сфере.

Интересы общества заключаются в использовании информации и информационной инфраструктуры для развития всех сфер общественной жизни.

Интересы государства в информационной сфере заключаются в использовании информации и информационной инфраструктуры для обеспечения государственной политики, защиты нравственных ценностей общества, обеспечения устойчивого функционирования информационной инфраструктуры, управления делами общества.

В соответствии с ранее упомянутым основным принципом обеспечение информационной безопасности является одной из наиболее важных задач в информационной сфере Российской Федерации. Решение этой задачи неразрывно связано с обеспечением безопасности национальных интересов в информационной сфере в целом.

В свою очередь, безопасность национальных интересов в информационной сфере определяется безопасностью объектов интересов, деятельности субъектов интересов по получению возможного обладания объектами интересов (деятельности по реализации интересов), которая осуществляется в рамках системы общественных отношений, о посредующих эту деятельность.

Обеспечение информационной безопасности Российской Федерации достигается разработкой и реализацией комплекса мероприятий, направленных на поддержание состояния защищенности национальных интересов Российской Федерации в различных сферах жизнедеятельности общества и государства. Особое место в системе этих мероприятий занимают организационные меры, способы и методы обеспечения информационной безопасности.

Однако прежде чем приступить к рассмотрению основ организационно-правового обеспечения информационной безопасности необходимо более глубоко раскрыть структуру, сущность и содержание понятия "обеспечение информационной безопасности".

В целях определения сущности и содержания понятия "обеспечение информационной безопасности" собственно информационная безопасность может быть определена как невозможность нанесения вреда свойствам объекта безопасности, которые в первую очередь характеризуются наличием информационной инфраструктуры и информации. По иному, информационная безопасность - состояние защищенности объекта безопасности от внешних и внутренних угроз.

В случае, когда объектом информационной безопасности является коммерческое предприятие, содержание понятия "информационная безопасность" заключается в защищенности интересов собственника информации, удовлетворяемых путем использования, обработки и применения информации, или связанных с защитой наиболее важных сведений, содержащихся в этой информации. Объектом безопасности в данном случае являются интересы собственника, представляющие собой совокупность информации, способной удовлетворить интересы собственника, и его действий по овладению этой информацией (ее сокрытием).

Следовательно, защита информационных ресурсов предприятия включает в себя деятельность руководства, должностных лиц и структурных подразделе-

ний предприятия по защите информации от несанкционированного доступа к информации, ее уничтожения, изменения и других опасных воздействий на защищаемую информацию.

Таким образом, обеспечение информационной безопасности есть совокупность деятельности по недопущению вреда свойствам объекта безопасности, обусловливаемым информацией и информационной инфраструктурой, а также средств и субъектов этой деятельности. Структура понятия "обеспечение информационной безопасности" представлена на рисунке 2.1.

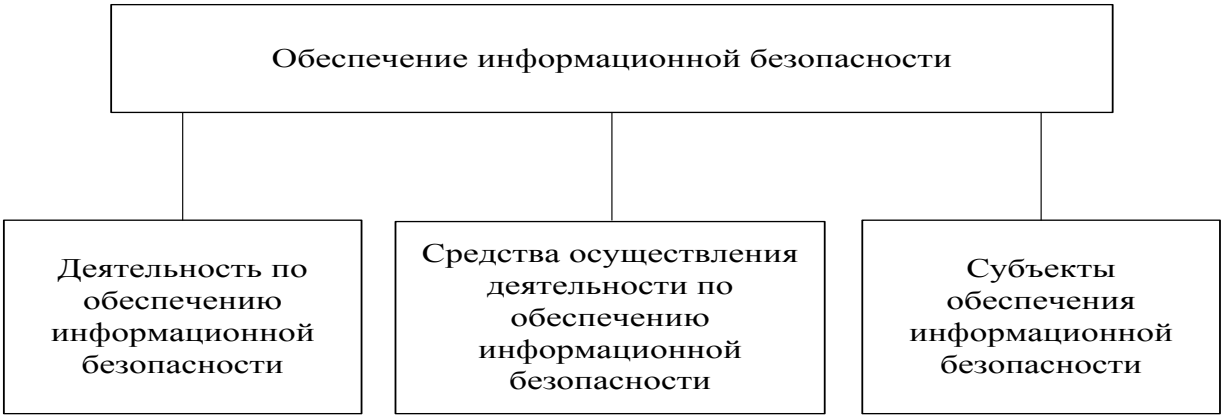

Рис. 2.1. Структура понятия "обеспечение информационной безопасности"

Деятельность по обеспечению информационной безопасности - комплекс планируемых и проводимых в целях защиты информационных ресурсов мероприятий, направленных на ликвидацию угроз информационной безопасности и минимизацию возможного ущерба, который может быть нанесен объекту безопасности вследствие их реализации.

Под субъектами обеспечения информационной безопасности понимаются государственные органы, предприятия, должностные лица, структурные подразделения, принимающие непосредственное участие в организации и проведении мероприятий по обеспечению информационной безопасности.

Средства, с помощью которых достигаются цели деятельности по обеспечению информационной безопасности, - это системы, объекты, способы, методы и иные механизмы непосредственного решения задач обеспечения информационной безопасности. Прежде всего, они представляют собой совокупность правовых и организационных средств обеспечения информационной безопасности.

Особую роль в системе средств обеспечения информационной безопасности, играют организационные средства. Основные виды организационных средств обеспечения информационной безопасности представлены на рисунке 2.2.

Наряду с организационными средствами обеспечения информационной безопасности в общей системе информационной безопасности важное место занимают и организационные методы. Доктрина информационной безопасности Российской Федерации[10] в целях обеспечения информационной безопасности нашего государства определяет следующие, наиболее важные из них:

- создание и совершенствование системы обеспечения информационной безопасности Российской Федерации;

[10] "Доктрина информационной безопасности Российской Федерации", утверждена Президентом РФ от 9.09.2000 г. № Пр-1895.

- усиление правоприменительной деятельности федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации, включая предупреждение и пресечение правонарушений в информационной сфере, а также выявление, изобличение и привлечение к ответственности лиц, совершивших преступления и другие правонарушения в этой сфере;

- сертификация средств защиты информации, лицензирование деятельности в области защиты государственной тайны, стандартизация способов и средств защиты информации;

- совершенствование системы сертификации телекоммуникационного оборудования и программного обеспечения автоматизированных систем обработки информации по требованиям информационной безопасности;

- контроль за действиями персонала в защищенных информационных системах, подготовка кадров в области обеспечения информационной безопасности Российской Федерации;

- формирование системы мониторинга показателей и характеристик информационной безопасности Российской Федерации в наиболее важных сферах жизни и деятельности общества и государства.

Рис. 2.2. Основные виды организационных средств обеспечения информационной безопасности

Вышеперечисленные организационные методы обеспечения информационной безопасности находят свое практическое применение в деятельности руководства и должностных лиц конкретного предприятия, на котором планируются и проводятся мероприятия по обеспечению информационной безопасности объектов информационной инфраструктуры, содержащих информацию, непосредственно подлежащую защите.

3. ОРГАНИЗАЦИОННЫЕ ОСНОВЫ ЗАЩИТЫ ИНФОРМАЦИИ

3.1. Основные принципы и условия организационной защиты информации

Организационная защита информации по своей сути является организационным началом, так называемым "ядром" в общей системе защиты конфиденциальной информации предприятия. От полноты и качества решения руководством предприятия организационных задач зависит эффективность решения проблем в данной области в целом.

Роль и место организационной защиты информации в общей системе мер, направленных на защиту конфиденциальной информации предприятия, определяются исходя из исключительной важности принятия руководством правильного и своевременного управленческого решения на основе действующего нормативно-методического аппарата, а также имеющихся в его распоряжении сил, средств, методов и способов защиты информации. Основные направления защиты информации представлены на рисунке 3.1.

Рис. 3.1. Основные направления защиты информации

Роль руководства предприятия в решении задач по защите информации трудно переоценить. Основными направлениями деятельности руководителя предприятия сегодня являются: планирование мероприятий по защите информации и персональный контроль за их выполнением, принятие решений по непосредственному доступу к конфиденциальной информации своих сотрудников и представителей других организаций; распределение обязанностей и задач между должностными лицами и структурными подразделениями; аналитическая работа и т.д.

Цель принимаемых руководством предприятия и должностными лицами организационных мер - исключение утечки информации и, таким образом, уменьшение или полное исключение возможности нанесения предприятию ущерба, к которому эта утечка может привести.

Система мер по защите информации в широком смысле слова должна строиться исходя из тех начальных условий и факторов, которые в свою очередь определяются состоянием устремленности разведок противника (действиями конкурента на рынке товаров и услуг), направленным на овладение информацией, подлежащей защите. Это правило действует как на государственном уровне, так и на уровне отдельного предприятия.

Таким образом, для раскрытия понятия "организационная защита информации", могут использоваться два, равных по своей сути, определения организационной зашиты информации.

Организационная защита информации - составная часть системы защиты информации, определяющая и вырабатывающая порядок и правила функционирования объектов защиты и деятельности должностных лиц в целях обеспечения защиты информации.

Организационно-правовая защита информации - регламентация производственной деятельности и взаимоотношений субъектов (сотрудников предприятия) на нормативно-правовой основе, исключающая или ослабляющая нанесение ущерба данному предприятию.

Первое из приведенных определений в большей степени показывает сущность организационной защиты информации. Второе - раскрывает ее структуру на уровне предприятия.

Вместе с тем, оба определения подчеркивают важность нормативно-правового регулирования вопросов защиты информации наряду с комплексным подходом к использованию в этих целях имеющихся сил и средств.

Основные направления организационной защиты информации приведены на рисунке 3.2.

Рис. 3.2. Основные направления организационной защиты информации

Таким образом, организационная защита информации сегодня является важнейшим элементом в общей системе защиты информации предприятия, с высокой эффективностью обеспечивающим ее защиту при условии соблюдения должностными лицами предприятия норм и правил защиты информации, определенных в соответствующих нормативно-методических документах.

Основными принципами организационной защиты информации являются следующие принципы: принцип комплексного подхода к решению задач защиты информации; принцип оперативности принятия управленческих решений; принцип персональной ответственности.

Принцип комплексного подхода заключается в использовании сил, средств, способов и методов защиты информации для решения поставленных за-

дач в зависимости от конкретной складывающейся ситуации и наличия факторов, ослабляющих или усиливающих угрозу возможной утечки конфиденциальной информации.

Принцип оперативности принятия управленческих решений существенно влияет на эффективность функционирования и гибкость системы защиты информации и отражает целеустремленность должностных лиц на решение задач защиты информации.

Принцип персональной ответственности заключается в наиболее эффективном и полном распределении сил структурных подразделений предприятия, участвующих в процессе защиты информации.

Среди основных условий организационной защиты информации можно выделить следующие:

- непрерывность всестороннего анализа состояния системы защиты информации с целью принятия своевременных мер по повышению ее эффективности;

- неукоснительное соблюдение должностными лицами и сотрудниками структурных подразделений предприятия установленных норм и правил защиты конфиденциальной информации.

При соблюдении вышеперечисленных условий будет обеспечено наиболее полное и качественное решение задач по защите конфиденциальной информации на предприятии.

3.2. Основные подходы и требования к организации системы защиты информации

Успешное решение комплекса задач по защите конфиденциальной информации не может быть достигнуто без создания единой основы, так называемого "активного кулака" предприятия, способного концентрировать все усилия, имеющиеся ресурсы для исключения утечки конфиденциальной информации и недопущения возможности нанесения ему ущерба.

Таким "кулаком" призвана стать система защиты информации на предприятии, создаваемая на нормативно-методической основе в данной области и отражающая все направления и специфику его деятельности.

Под системой защиты информации понимается совокупность органов защиты информации (структурных подразделений или должностных лиц предприятия), используемых ими средств и методов защиты информации, а также мероприятий, планируемых и проводимых в этих целях. Структура системы защиты информации приведена на рисунке 3.3.

Для решения организационных задач по созданию и функционирования системы защиты информации используются несколько основных подходов, которые вырабатываются на основе существующей нормативно-правовой базы и с учетом методических разработок по тем или иным направлениям защиты конфиденциальной информации.

Один из основных подходов к созданию системы защиты информации заключается во всестороннем анализе состояния защищенности информационных ресурсов предприятия с учетом устремленности конкурирующих организаций к овладению конфиденциальной информацией и, тем самым, нанесению ущерба предприятию. Важным элементом анализа является работа по определению перечня защищаемых информационных ресурсов с учетом особенностей их распо-

ложения (размещения) и доступа к ним различных категорий сотрудников (работников других предприятий).

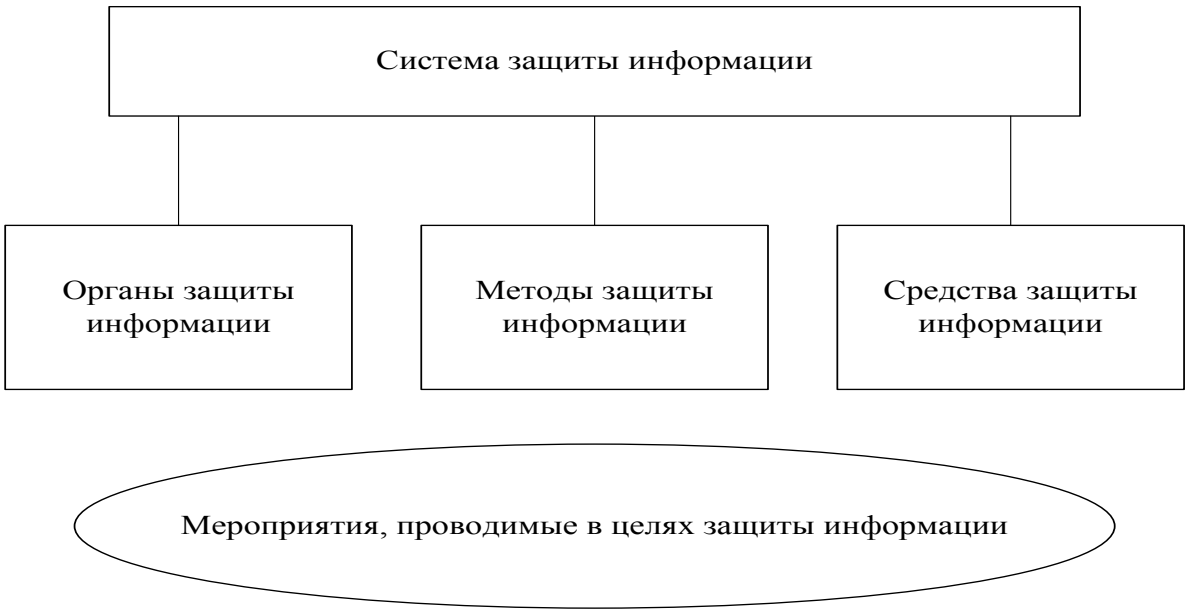

Рис. 3.3. Структура системы защиты информации

Работу по проведению такого анализа непосредственно возглавляет руководитель предприятия и его заместители по направлениям деятельности. Изучение защищенности информационных ресурсов основывается на положительном и отрицательном опыте работы предприятия, накопленном в течение последних нескольких лет, а также наработанных деловых связях и контактах предприятия с организациями, осуществляющими аналогичные виды деятельности.

При создании системы защиты информации, в первую очередь, учитываются наиболее важные, приоритетные направления деятельности предприятия, требующие особого внимания. Предпочтение также отдается новым, перспективным направлениям деятельности предприятия, связанным с научными исследованиями, новейшими технологиями, формирующими интеллектуальную собственность, а также развивающимся международным связям. На этой основе формируется перечень возможных угроз информации, подлежащей защите, и определяются предполагаемые к использованию в этих целях конкретные силы, средства, способы и методы ее защиты.

К организации системы защиты информации с позиции системного подхода выдвигается ряд требований, определяющих ее целостность, стройность и эффективность.

Система защиты информации должна отвечать совокупности следующих основных требований, то есть быть:

централизованной - соответствующей эффективному процессу управления системой со стороны руководителя и ответственных должностных лиц по направлениям деятельности предприятия;

плановой - объединяющей усилия различных должностных лиц и структурных подразделений при их участии в организации и обеспечении выполнения задач, стоящих перед предприятием;

конкретной и целенаправленной - защите должны подлежать абсолютно конкретные информационные ресурсы, представляющие интерес для конкурирующих организаций;

активной - обеспечивать защиту информации с достаточной степенью настойчивости и возможностью концентрации усилий на наиболее важных направлениях деятельности предприятия;

надежной и универсальной - охватывать весь комплекс деятельности предприятия, связанной с созданием и обменом информацией.

3.3. Основные силы и средства, используемые для организации защиты информации

Одним из важнейших факторов, оказывающих существенное влияние на эффективность системы защиты конфиденциальной информации, является совокупность сил и средств предприятия, используемых для организации защиты информации и непосредственно участвующих в этом процессе.

Силы и средства различных предприятий отличаются по структуре, характеру и порядку использования. Предприятия, осуществляющие работу с конфиденциальной информацией и решающие задачи по ее защите на постоянной основе, то есть в каждодневной деятельности, вынуждены с этой целью создавать самостоятельные структурные подразделения и использовать высокоэффективные средства защиты информации.

Предприятиями, осуществляющими эпизодическую работу с конфиденциальной информацией, в силу ее небольших объемов, вместо создания вышеупомянутых подразделений в штаты своих предприятий могут включаться самостоятельные должности специалистов по защите информации.

Наряду с этим, данные предприятия на договорной основе могут использовать потенциал более крупных предприятий, имеющих необходимое количество квалифицированных сотрудников и высокоэффективные средства защиты информации. Эти вопросы регулируются нормативными актами, определяющими порядок оказания услуг в данной области.

Ведущую роль в организации защиты информации на предприятии играет руководитель предприятия, а также его заместитель, непосредственно возглавляющий эту работу.

Руководитель предприятия в соответствии с законодательством несет персональную ответственность за организацию и осуществление необходимых мероприятий, направленных на исключение утечки сведений, отнесенных к конфиденциальной информации, и утрат носителей информации.

Руководитель предприятия при организации работ по защите информации обязан:

- знать фактическое состояние дел по этим вопросам, организовывать постоянную работу по выявлению и закрытию возможных каналов утечки конфиденциальной информации;
- определять обязанности и задачи должностным лицам и структурным подразделениям предприятия в этой области;
- предъявлять высокую требовательность к сотрудникам предприятия в вопросах сохранности сведений конфиденциального характера;
- оценивать деятельность должностных лиц по защите информации и эффективность проводимых в целях защиты соответствующих сведений мероприятий.

Заместитель руководителя предприятия обязан постоянно изучать все стороны и направления деятельности предприятия с целью принятия своевремен-

ных мер по защите информации; руководить работой службы безопасности (структурных подразделений по защите государственной тайны), а также выполнять другие функции по организации защиты информации в ходе проведения предприятием всех видов работ.

В структуре предприятий с целью организации работ по защите информации могут создаваться следующие основные виды структурных подразделений:

- режимно-секретные;
- подразделения по противодействию иностранным техническим разведкам и технической защите информации;
- подразделения криптографической защиты информации;
- мобилизационные;
- подразделения охраны и пропускного режима.

Функции, возлагаемые на вышеперечисленные подразделения, определяются решением (приказом) руководителя предприятия и отражаются в соответствующих положениях. Более подробно указанные функции, а также задачи, решаемые данными подразделениями, будут рассмотрены в последующих разделах учебного пособия.

По решению руководителя предприятия вышеупомянутые подразделения могут быть структурно объединены в службу режима предприятия, руководитель которой наделяется статусом заместителя руководителя предприятия, и полномочиями должностного лица, имеющего право осуществлять непосредственное руководство деятельностью всех подразделений предприятия, если их деятельность связана с использованием информации, отнесенной к конфиденциальной информации (государственной тайне) и подлежащей защите.

Характерной особенностью функционирования режимно-секретного подразделения, мобилизационного подразделения и подразделения по противодействию иностранным техническим разведкам и технической защите информации является то, что они создаются на предприятиях, выполняющих работы с использованием сведений, составляющих государственную тайну.

Режимно-секретное подразделение является основным структурным подразделением предприятия и решает задачи организации, координации и контроля деятельности других структурных подразделений (должностных лиц) по обеспечению защиты сведений, составляющих государственную тайну. На предприятиях, не выполняющих работы со сведениями, составляющими государственную тайну, для решения аналогичных задач создается и функционирует служба защиты информации (служба безопасности).

Подразделение по противодействию иностранным техническим разведкам и технической защите информации решает задачи организации и проведения комплекса технических мероприятий, направленных на исключение или существенное затруднение добывания иностранными разведками с помощью технических средств сведений, являющихся конфиденциальной информацией и подлежащих защите.

Подразделение криптографической защиты информации создается с целью закрытия каналов утечки конфиденциальной информации при ее передаче по открытым каналам (линиям) связи с использованием технических средств, а также использовании локальных вычислительных сетей, имеющих выход за пределы территории предприятия.

Подразделение охраны и пропускного режима создается с целью предотвращения несанкционированного (бесконтрольного) пребывания на территории и объектах предприятия посторонних лиц и транспорта, нанесения ущерба предприятию путем краж (хищений) с территории предприятия материальных средств и иного имущества.

Мобилизационное подразделение решает задачи всесторонней подготовки предприятия к работе в условиях военного времени, призыва и поступления мобилизационных людских и материальных ресурсов.

Кроме вышеперечисленных подразделений предприятия к работе по организации защиты информации могут привлекаться и иные структурные подразделения предприятия, основным направлением деятельности которых защита информации не является. Это - кадровые органы, органы юридической службы, органы психологической работы. Особо необходимо отметить участие в организации защиты информации производственных, так называемых "тематических" подразделений, непосредственно создающих продукцию, товары и услуги, и, в этой связи, непосредственно взаимодействующих с другими предприятиями и органами государственной власти.

При проведении работ по организации защиты информации используются и возможности различных нештатных подразделений предприятия, в том числе коллегиальных органов (комиссий), создаваемых для решения специфических задач в этой области. Это - постоянно действующая техническая комиссия, экспертная комиссия, комиссия по рассекречиванию носителей конфиденциальной информации, комиссия по категорированию объектов автоматизации и другие. Функции, возлагаемые на данные комиссии, будут рассмотрены в последующих главах настоящего учебного пособия, а также в ходе изучения других дисциплин.

Однако, для достижения наиболее эффективного результата при решении задач защиты конфиденциальной информации, наряду с использованием возможностей вышеупомянутых штатных и нештатных подразделений, необходимо комплексное применение имеющихся на предприятии средств защиты конфиденциальной информации.

Под средствами защиты информации понимаются технические, криптографические, программные и другие средства и системы, разработанные и предназначенные для защиты конфиденциальной информации, специальные средства, в которых они реализованы, а также средства, устройства и системы контроля эффективности защиты информации.

Технические средства защиты информации - устройства (приборы), предназначенные для обеспечения защиты информации, исключения ее утечки, создания помех (препятствий) техническим средствам доступа к информации, подлежащей защите.

Криптографические средства защиты информации - средства (устройства), обеспечивающие защиту конфиденциальной информации путем ее криптографического преобразования (шифрования).

Программные средства защиты информации - системы защиты средств автоматизации (персональных электронно-вычислительных машин и их комплексов) от внешнего (постороннего) воздействия или вторжения.

Комплексное применение средств защиты конфиденциальной информации невозможно без четко определенной стратегии защиты информации или, методов защиты информации.

Методы защиты информации - выборочно применяемые универсальные и специфические способы (приемы, меры, мероприятия) реализации элементов системы защиты информации и входящих в них содержательных частей для формирования комплексной и индивидуальной структуры данной системы.

Общие методы защиты информации разделяются на правовые, организационно-технические и экономические.

Содержание правовых методов защиты информации направлено на решение следующих задач:

- разработку, совершенствование и обеспечение функционирования механизмов отнесения сведений к информации ограниченного доступа, засекречивания (рассекречивания) носителей информации, составляющей государственную тайну и иную охраняемую законом тайну, установления (снятия) ограничительных грифов для носителей конфиденциальной информации;
- определение перечней сведений, отнесенных к государственной (коммерческой) тайне;
- установление правового режима работы органов защиты информации;
- установление порядка доступа и допуска должностных лиц и граждан к государственной тайне и т.д.

В организационно-технических методах защиты информации рассмотрим только ее организационную составляющую, т.к. технические и экономические методы защиты информации выходят за рамки данного учебного пособия и рассматриваться не будут.

Соотношение правового обеспечения защиты информации и организационных мер ставит в зависимость деятельность по организации процесса защиты и администрированию некоторых защитных процедур от законодательства. Законодательная система является основой разработки организационных мероприятий, и предлагает общие идеи и принципы, выраженные в нормах права, для планирования и организации деятельности, направленной на защиту конкретных сведений. В свою очередь, организационные мероприятия являются "приемниками" правовых норм, развивают и уточняют их для конкретных условий, объектов и должностных лиц. С позиций системного подхода организация позволяет упорядочить, систематизировать любую деятельность.

Организационные методы защиты информации подразделяются по следующим классам:

- организация и соблюдение определенного порядка управленческой деятельности предприятия, направленная снижение риска утраты, утечки, модификации сведений конфиденциального характера;
- установление и соблюдение требований по организации и ведению конфиденциального делопроизводства, в том числе по размещению, оборудованию и охране;
- работа по ограничению (разграничению) круга должностных лиц предприятия по доступу к государственной тайне и конфиденциальной информации;
- осуществление принципа персональной ответственности должностных лиц за сохранность доверенной информации;

- организация подбора лиц, работающих с важной информацией их воспитание и обучение;

- систематический контроль за соблюдением режима защиты данных и оказание помощи подчиненным структурным подразделениям;

- мероприятия по сокращению оборота носителей секретной и конфиденциальной информации, систематический отбор и уничтожение ненужных носителей.

Таким образом, эффективное решение задач организации защиты информации невозможно без применения комплекса имеющихся в распоряжении руководителя предприятия методов защиты информации и соответствующих сил и средств.

4. ОТНЕСЕНИЕ СВЕДЕНИЙ К КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ. ЗАСЕКРЕЧИВАНИЕ И РАССЕКРЕЧИВАНИЕ СВЕДЕНИЙ

4.1. Отнесение сведений к различным видам конфиденциальной информации

В соответствии с Федеральным законом РФ "Об информации, информационных технологиях и защите информации"[11] под информацией понимаются сведения (сообщения, данные) независимо от формы их представления.

При регулировании отношений, возникающих при осуществлении права на поиск, получение, передачу, производство и распространение информации; обеспечении ее защиты используются следующие основные понятия:

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

доступ к информации - возможность получения информации и ее использования;

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

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

распространение информации - действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц.

Под документированной информацией при этом понимается зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или в установленных законодательством государства случаях ее материальный носитель.

Основными принципами правового регулирования отношений, возникающих в сфере информации, информационных технологий и защиты информации в России являются:

[11] Федеральный закон РФ от 27.07.2006 г. № 149-ФЗ "Об информации, информационных технологиях и защите информации".

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

- установление ограничений доступа к информации только федеральными законами;

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

В зависимости от категории доступа к информации она подразделяется на общедоступную информацию, а также на информацию, доступ к которой ограничен федеральными законами (информация ограниченного доступа).

К общедоступной информации относятся общеизвестные сведения и иная информация, доступ к которой не ограничен.

Общедоступная информация может использоваться любыми лицами по их усмотрению при соблюдении установленных федеральными законами ограничений в отношении распространения такой информации.

Статья 29 Конституции РФ[12] определяет право каждого гражданина свободно искать, получать, передавать, производить и распространять информацию любым законным способом.

На основании Федерального закона РФ "Об информации, информационных технологиях и защите информации" информация может свободно использоваться любым лицом и передаваться одним лицом другому лицу, если федеральными законами не установлены ограничения доступа к информации либо иные требования к порядку ее предоставления или распространения. Граждане (физические лица) и организации (юридические лица) вправе осуществлять поиск и получение любой информации в любых формах и из любых источников при условии соблюдения требований, установленных законодательством Российской Федерации.

Ограничение доступа к информации в соответствии со статьей 55 Конституции РФ и статьей 9 Федерального закона РФ "Об информации, информационных технологиях и защите информации" устанавливается федеральными законами в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства. При этом обязательным является соблюдение конфиденциальности информации, доступ к которой ограничен.

Таким образом, одним из наиболее важных аспектов в области регулирования отношений в сфере защиты информации является отнесение информации к различным категориям, так называемым видам тайн или ограничений.

В настоящее время федеральные законы определяют лишь условия и порядок отнесения информации к государственной тайне[13] и коммерческой тайне[14]. Ограничения по доступу к иной конфиденциальной информации (иным видам тайн) федеральными законами не установлены.

В РФ определен такой вид конфиденциальной информации, как персональные данные. Федеральным законом РФ "О персональных данных"[15] определен исчерпывающий перечень информации, относящейся к персональным дан-

[12] Конституция РФ, принята на всенародном голосовании 12.12.1993 г.
[13] Закон РФ от 21.07.1993 г. № 5485-1 "О государственной тайне".
[14] Федеральный закон РФ от 29.07.2004 г. № 98-ФЗ "О коммерческой тайне".
[15] Федеральный закон РФ от 27.07.2006 г. № 152-ФЗ "О персональных данных".

ным физического лица (см. приложение 1), а статьями 85 - 90 Трудового кодекса РФ[16] определен порядок работы с персональными данными, включая и мероприятия по их защите (см. приложение 12). За отказ в предоставлении гражданину информации, касающейся его персональных данных, а также за нарушение установленного Федеральным законом РФ "О персональных данных" порядка сбора, хранения, использования или распространения персональных данных предусмотрена административная ответственность по статьям 5.39 и 13.11 (соответственно) Кодекса РФ об административных правонарушениях[17] (см. приложение 10).

Вопросы отнесения информации к служебной информации ограниченного распространения изложены в "Положении о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти"[18].

Таким образом, основываясь на вышеупомянутых положениях статьи 55 Конституции РФ, право на доступ граждан к информации может быть ограничен только в отношении информации, отнесенной к государственной или коммерческой тайне.

Статья 7 Закона РФ "О государственной тайне" и статья 5 Федерального закона РФ "О коммерческой тайне" содержат исчерпывающие перечни сведений, которые не могут быть отнесены к государственной (см. приложение 2) и коммерческой (см. приложение 3) тайне соответственно. Следовательно, и доступ к этим сведениям граждан должен осуществляться без каких-либо ограничений.

Без ограничений граждане допускаются и к сведениям, перечисленным в пункте 1.3. "Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти", которые руководителями органов государственной власти, предприятий и организаций не могут быть отнесены к данному виду информации.

Отнесение информации к коммерческой тайне законом возложено на ее обладателя, то есть на юридическое или физическое лицо. Исключительно обладатель коммерческой тайны имеет право вводить и отменять режим коммерческой тайны, устанавливать меры по ее защите, разрешать доступ лиц к данной информации. Обладатель коммерческой тайны наделен полномочиями и правами по формированию перечня информации, отнесенной к коммерческой тайне. Он непосредственно принимает решение как о допуске гражданина к информации, являющейся коммерческой тайной, так и по другим вопросам, связанным с коммерческой тайной предприятия. Практический механизм отнесения информации к коммерческой тайне достаточно прост, он основывается исключительно на административном решении ее правообладателя, как правило, руководителя предприятия.

В настоящее время в Российской Федерации законодательно определено около 20 видов конфиденциальной информации[19], основные из них представлены в приложении 4.

---

[16] Принят Федеральным законом РФ от 30.12.2001 г. № 197-ФЗ.

[17] Принят Федеральным законом РФ от 30.12.2001 г. № 195-ФЗ.

[18] Утверждено постановлением Правительства РФ от 3.11.1994 г. № 1233.

[19] Указ Президента РФ от 06.03.1997 г. № 188 "Об утверждении Перечня сведений конфиденциального характера".

Поэтому основное внимание на страницах учебного пособия будет уделено рассмотрению вопросов, связанных с отнесением сведений к государственной и коммерческой тайне, засекречиванием сведений и их носителей[20], а также допуском должностных лиц и граждан к государственной и коммерческой тайне.

4.2. Грифы секретности и реквизиты носителей сведений, составляющих государственную тайну

В Российской Федерации установлены три степени секретности сведений, составляющих государственную тайну, и соответствующие этим степеням грифы секретности для носителей указанных сведений: "особой важности", "совершенно секретно" и "секретно" (см. рисунок 4.1).

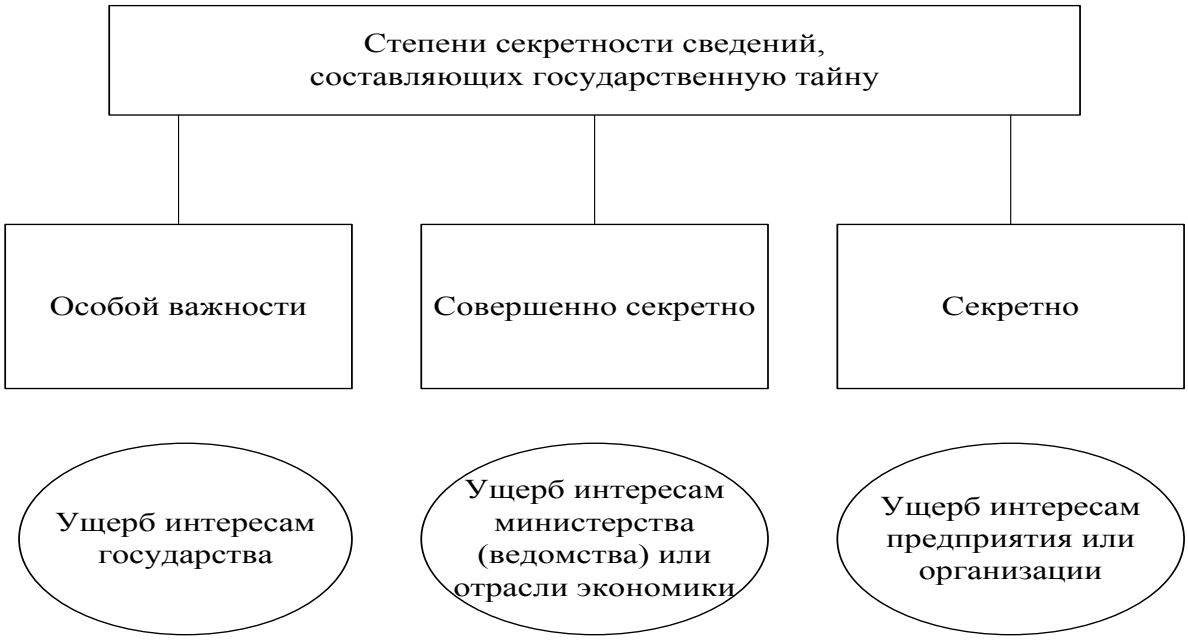

Рис. 4.1. Степени секретности сведений, составляющих государственную тайну

Конкретная степень секретности сведений, составляющих государственную тайну, должна соответствовать степени тяжести ущерба, который может быть нанесен безопасности Российской Федерации вследствие распространения указанных сведений. Она определяется руководителями органов государственной власти в развернутых перечнях сведений, подлежащих засекречиванию.

Сведения, отнесенные к государственной тайне, по степени секретности подразделяются на сведения особой важности, совершенно секретные и секретные.

К сведениям ***особой важности*** следует относить сведения в области военной, внешнеполитической, экономической, научно-технической, разведывательной, контрразведывательной и оперативно-розыскной 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, разве-

[20] 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.

дывательной, контрразведывательной и оперативно-розыскной 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 или организации в военной, внешнеполитической, экономической, научно-технической, разведывательной, контрразведывательной или оперативно-розыскной области деятельности.

Носителям сведений, составляющих государственную тайну, присваивается конкретный гриф секретности.

С целью идентификации носителей сведений, составляющих государственную тайну, определения их принадлежности, обеспечения их учета и сохранности, на них наносятся реквизиты, 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 организации развернутого перечня сведений, подлежащих засекречиванию;
- об органе государственной власти, предприятии или организации, осуществивших засекречивание носителя;
- о регистрационном номере;
- о дате или условии рассекречивания включенных в носитель сведений, составляющих государственную тайну, либо о событии, после наступления которого сведения будут рассекречены.

При невозможности нанесения таких реквизитов на носитель сведений, составляющих государственную тайну (крупногабаритное изделие, изделие, изготовленное из материала, на который нанести реквизиты невозможно), 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 настоящем разделе 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 РФ.

4.3. Грифы секретности и реквизиты носителей сведений, составляющих коммерческую тайну

В Российской Федерации установлена одна степень конфиденциальности сведений, составляющих коммерческую тайну, и соответствующий гриф "Коммерческая тайна"[21].

С целью идентификации носителей сведений, составляющих коммерческую тайну, определения их принадлежности, обеспечения их учета и сохранности, на них наносятся реквизиты, включающие следующие данные:

- гриф "Коммерческая тайна";
- об обладателе коммерческой информации (для юридических лиц - полное наименование и место нахождения, для индивидуальных предпринимателей - фамилия, имя, отчество гражданина, являющегося индивидуальным предпринимателем, и место жительства);
- также необходимо указать регистрационный номер носителя информации, составляющей коммерческую тайну.

При невозможности нанесения таких реквизитов на носитель сведений, составляющих государственную тайну (крупногабаритное изделие, изделие, изготовленное из материала, на который нанести реквизиты невозможно), эти данные указываются в сопроводительной документации на этот носитель.

4.4. Отнесение сведений к государственной тайне. Засекречивание сведений и их носителей

Под отнесением сведений к государственной тайне и их засекречиванием понимается введение, в предусмотренном Законом РФ "О государственной тайне" порядке для сведений, составляющих государственную тайну, ограничений на их распространение и на доступ к их носителям.

Основными принципами отнесения сведений к государственной тайне и их засекречивания являются принципы законности, обоснованности и своевременности.

Законность отнесения сведений к государственной тайне и их засекречивания заключается в соответствии засекречиваемых сведений положениям статей 5 и 7 Закона РФ "О государственной тайне" (см. приложение 2) и законодательству РФ о государственной тайне. Обоснованность отнесения сведений к государственной тайне и их засекречивания заключается в установлении путем экспертной оценки целесообразности засекречивания конкретных сведений, вероятных экономических и иных последствий этого акта исходя из баланса жизненно важных интересов государства, общества и граждан.

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

Отнесение сведений к государственной тайне осуществляется в соответствии с их отраслевой, ведомственной или программно-целевой принадлежностью порядком, определенным Законом РФ "О государственной тайне".

---

[21] Сведения, которым присваивается гриф "Коммерческая тайна" должны быть включены в "Перечень информации, составляющей коммерческую тайну" предприятия.

Обоснование необходимости отнесения сведений к государственной тайне в соответствии с упомянутыми принципами засекречивания сведений возлагается на органы государственной власти, предприятия, учреждения и организации, которыми эти сведения получены (разработаны).

Отнесение сведений к государственной тайне осуществляется в соответствии с "Перечнем сведений, составляющих государственную тайну"[22], руководителями органов государственной власти, включенными в "Перечень должностных лиц, наделенных полномочиями по отнесению сведений к государственной тайне"[23].

При этом указанные должностные лица несут персональную ответственность за принятые ими решения о целесообразности отнесения конкретных сведений к государственной тайне.

Структура "Перечня сведений, составляющих государственную тайну", представлена на рисунке 4.2.

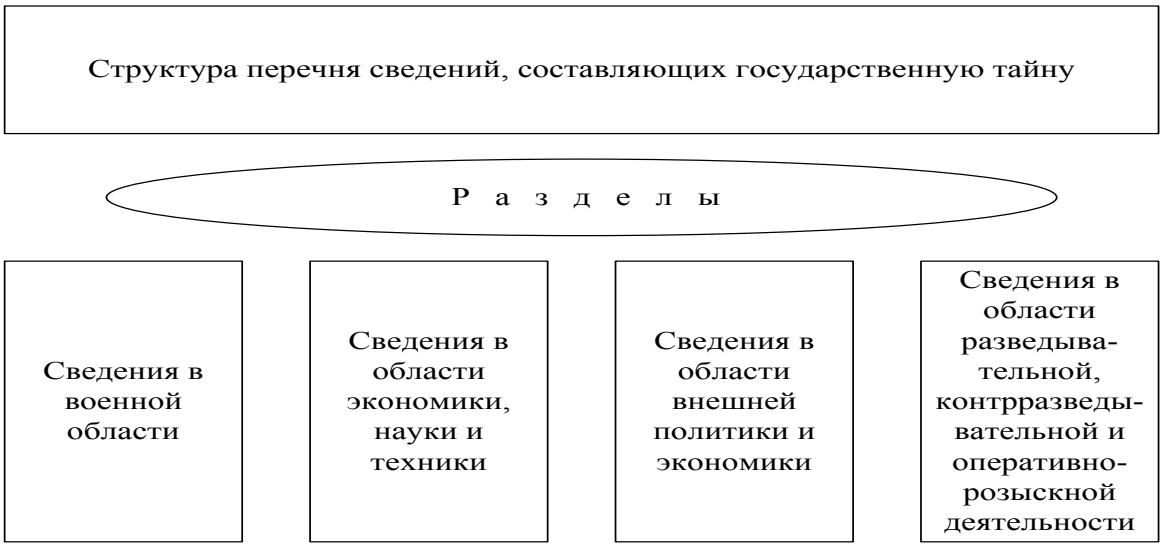

Рис. 4.2. Структура перечня сведений, составляющих государственную тайну

Вместе с тем, в соответствии со статьей 7 Закона РФ "О государственной тайне", 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;
- о состоянии экологии, здравоохранения, санитарии, демографии, образования, культуры, сельского хозяйства, а также о состоянии преступности;
- о привилегиях, компенсациях и льготах, предоставляемых государством гражданам, должностным лицам, предприятиям, учреждениям и организациям;
- о фактах нарушения прав и свобод человека и гражданина;
- о размерах золотого запаса и государственных валютных резервах Российской Федерации;
- о состоянии здоровья высших должностных лиц Российской Федерации;
- о фактах нарушения законности органами государственной власти и их должностными лицами.

[22] Статья 5 Закона РФ от 21.07.1993 г. № 5485-1 "О государственной тайне".
[23] Утвержден распоряжением Президента РФ от 16.04.2005 г. № 151-рп.

Руководители и 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.

В соответствии "Перечнем сведений, составляющих государственную тайну", Межведомственная комиссия по защите государственной тайны[24], являющаяся органом, осуществляющим единую государственную политику в данной области[25], на основании предложений государственных органов формирует "Перечень сведений, отнесенных к государственной тайне"[26]. Этот перечень является открытым, в нем указываются органы государственной власти, наделяемые полномочиями по распоряжению данными сведениями.

Упомянутыми органами государственной власти, руководители которых наделены полномочиями по отнесению сведений к государственной тайне, в соответствии с "Перечнем сведений, отнесенных к государственной тайне", разрабатываются развернутые перечни сведений, подлежащих засекречиванию, которые действуют в данных государственных органах.

В них включаются конкретные сведения, полномочиями по распоряжению которыми наделены указанные органы, и устанавливается конкретная степень их секретности. Развернутые перечни сведений, подлежащих засекречиванию, в зависимости от их содержания могут быть открытыми или закрытыми (ограниченными для распространения).

Порядок разработки развернутых перечней и правила отнесения сведений к конкретным степеням секретности установлены "Правилами отнесения сведений, составляющих государственную тайну, к различным степеням секретности"[27].

Основанием для засекречивания сведений и их носителей, разработанных в органе государственной власти или на предприятии (в организации), является соответствие этих сведений положениям действующего в данном органе государственной власти (на предприятии, в организации) развернутого перечня сведений, подлежащих засекречиванию. При принятии решения о засекречивании сведений их носителям присваивается соответствующий гриф секретности.

В случае невозможности идентификации данных сведений со сведениями, включенными в вышеупомянутый перечень, руководители (должностные лица) органов государственной власти (предприятий, организаций) обязаны обеспечить их предварительное засекречивание в соответствии с предполагаемой степенью секретности и присвоить их носителям гриф секретности.

Эти руководители в месячный срок после засекречивания сведений (их носителей) направляют в адрес должностного лица, утвердившего указанный развернутый перечень сведений, подлежащих засекречиванию, предложения по его дополнению (изменению).

---

[24] Образована Указом Президента РФ от 8.11.1995 г. № 1108 "О Межведомственной комиссии по защите государственной тайны".

[25] Решением Межведомственной комиссии по защите государственной тайны от 17.06.1998 г. № 33 утверждена "Концепция защиты государственной тайны в Российской Федерации".

[26] Указ Президента РФ от 30.11.1995 г. № 1203 "Об утверждении Перечня сведений, отнесенных к государственной тайне".

[27] Утверждены постановлением Правительства РФ от 4.09.1995 г. № 870.

Должностные лица, утвердившие действующий перечень, обязаны в течение трех месяцев организовать экспертную оценку поступивших предложений и принять решение по дополнению (изменению) действующего перечня или снятию предварительно присвоенного сведениям грифа секретности.

4.5. Основания и порядок рассекречивания сведений и их носителей

Под рассекречиванием сведений, составляющих государственную тайну, и их носителей в соответствии со статьей 13 Закона РФ "О государственной тайне" понимается снятие ранее введенных в установленном порядке ограничений на их распространение и на доступ к их носителям.

Основаниями для рассекречивания сведений являются: взятие на себя Российской Федерацией международных обязательств по открытому обмену сведениями, составляющими в Российской Федерации государственную тайну; или изменение объективных обстоятельств, вследствие которых дальнейшая защита сведений, составляющих государственную тайну, является нецелесообразной.

В соответствии с Законом РФ "О государственной тайне" срок засекречивания сведений, составляющих государственную тайну, не должен превышать 30 лет. В исключительных случаях этот срок может быть продлен по заключению Межведомственной комиссии по защите государственной тайны.

Правом изменения действующих в органах государственной власти, на предприятиях и в организациях перечней сведений, подлежащих засекречиванию, наделяются утвердившие их руководители органов государственной власти. Эти руководители несут персональную ответственность за обоснованность принятых ими решений по рассекречиванию сведений, составляющих государственную тайну, ранее включенных в вышеупомянутые перечни.

В случае если решения указанных руководителей по рассекречиванию сведений, составляющих государственную тайну, влекут за собой изменения соответствующих положений (пунктов) "Перечня сведений, отнесенных к государственной тайне", они в установленном порядке подлежат согласованию с Межведомственной комиссией по защите государственной тайны, которая наделена правом приостанавливать или опротестовывать эти решения.

Органы государственной власти, руководители которых наделены полномочиями по отнесению сведений к государственной тайне, обязаны периодически, но не реже чем через каждые 5 лет, пересматривать содержание разработанных и утвержденных данными руководителями развернутых перечней сведений, подлежащих засекречиванию, в части обоснованности засекречивания сведений и их соответствия ранее установленной степени секретности.

Носители сведений, составляющих государственную тайну, рассекречиваются не позднее сроков, установленных при их засекречивании. До истечения этих сроков носители подлежат рассекречиванию, если изменены положения действующего в данном органе государственной власти, на предприятии, в учреждении и организации развернутого перечня, на основании которых они были засекречены.

В исключительных случаях право продления первоначально установленных сроков засекречивания носителей сведений, составляющих государственную тайну, предоставляется руководителям государственных органов, наделенным полномочиями по отнесению соответствующих сведений к государственной

тайне, на основании заключения назначенной ими в установленном порядке экспертной комиссии.

Руководители органов государственной власти, предприятий и организаций имеют право рассекречивать носители сведений, необоснованно засекреченные подчиненными им должностными лицами (руководителями предприятий или организаций).

Рассекречивание носителей сведений, составляющих государственную тайну, находящихся на хранении в закрытых фондах государственных архивов России осуществляется организациями-фондообразователями или их правопреемниками, а в случае их ликвидации - в соответствии с решением Межведомственной комиссии по защите государственной тайны.

В отдельных случаях, рассекречивание носителей сведений, составляющих государственную тайну, может производиться руководителями архивов, в которых они хранятся, при делегировании им таких полномочий организацией-фондообразователем или ее преемником[28].

В случае ликвидации организации-фондообразователя и отсутствия ее правопреемника вопрос о порядке рассекречивания носителей сведений, составляющих государственную тайну, рассматривается Межведомственной комиссией по защите государственной тайны.

После принятия решения о рассекречивании сведений, составляющих государственную тайну, и их носителей, реквизиты, ранее нанесенные на эти носители, в установленном порядке с них снимаются. С целью своевременного и одновременного снятия указанных реквизитов со всех экземпляров рассекреченных носителей, орган государственной власти или организация, непосредственно реализующие соответствующее решение руководителя, письменно извещают об этом решении все организации, в которых находятся (хранятся) экземпляры данного носителя.

4.6. Отнесение сведений к коммерческой тайне

Под отнесением сведений к коммерческой тайне понимается введение в предусмотренном Законом РФ "О коммерческой тайне" порядке для сведений, составляющих коммерческую тайну, ограничений на их распространение и на доступ к их носителям.

Основными принципами отнесения сведений к коммерческой тайне и их засекречивания являются принципы законности, обоснованности и своевременности.

Законность отнесения сведений к коммерческой тайне заключается в соответствии засекречиваемых сведений положениям статей 5 и 7 Закона РФ "О коммерческой тайне" (см. приложение 3) и законодательству РФ о сведениях конфиденциального характера[29].

К сведениям конфиденциального характера относятся:

---

[28] Особенности рассекречивания архивных документов Правительства СССР определены постановлением Правительства РФ от 20.02.1995 г. № 170 "Об установлении порядка рассекречивания и продления сроков засекречивания архивных документов Правительства СССР".

[29] Указ Президента РФ от 06.03.1997 г. № 188 "Об утверждении Перечня сведений конфиденциального характера".

1. Сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (персональные данные[30]), за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях.

2. Сведения, составляющие тайну следствия и судопроизводства.

3. Служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом РФ[31] и федеральными законами (служебная тайна[32]).

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

5. Сведения, связанные с коммерческой деятельностью, доступ к которым ограничен в соответствии с Гражданским кодексом РФ и федеральными законами (коммерческая тайна[33]).

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

Порядок присвоения сведениям грифа "Коммерческая тайна" и его снятия производится правообладателем этих сведений лишь на основании своего субъективного представления о степени их актуальности (неактуальности) при условии, что эти сведения предварительно включены в "Перечень информации, составляющей коммерческую тайну".

Как правило, в "Перечень информации, составляющей коммерческую тайну" включают следующие сведения:

1. Сведения о структуре и масштабах производства, производственных мощностях, типе и размещении оборудования, запасах сырья, материалов, комплектующих и готовой продукции.

2. Сведения о применяемых оригинальных методах управления предприятием. Сведения о подготовке, принятии и исполнении отдельных решений руководства предприятия по коммерческим, организационным, научно-техническим и иным вопросам.

3. Сведения о планах расширения или свертывания производства различных видов продукции и их технико-экономических обоснованиях. Также сведения о планах инвестиций, закупок и продаж.

4. Сведения о фактах проведения, целях, предмете и результатах совещаний и заседаний органов управления предприятия.

5. Сведения о кругообороте средств организации, финансовых операциях, состоянии банковских счетов предприятия и проводимых операциях, об уровне доходов предприятия, о состоянии кредита предприятия (пассивы и активы). Главная книга предприятия.

6. Сведения о применяемых предприятием оригинальных методах изучения рынка (маркетинга). Сведения о результатах изучения рынка, содержащие оценки состояния и перспектив развития рыночной конъюктуры. Сведения о

---

[30] Федеральный закон РФ от 27.07.2006 г. № 152-ФЗ "О персональных данных".

[31] Статья 139 Гражданского кодекса РФ (часть первая от 30.11.1994 г. № 51-ФЗ).

[32] Федеральный закон РФ "О служебной тайне" на момент выхода пособия еще не принят.

[33] Федеральный закон РФ от 29.07.2004 г. № 98-ФЗ "О коммерческой тайне".

рыночной стратегии предприятия, о применяемых предприятием оригинальных методах осуществления продаж, об эффективности коммерческой деятельности предприятия.

7. Обобщенные сведения о внутренних и зарубежных заказчиках, подрядчиках, поставщиках, потребителях, покупателях, компаньонах, спонсорах, посредниках, клиентах и других партнерах, состоящих в деловых отношениях с предприятием.

8. Обобщенные сведения о внутренних и зарубежных предприятиях как потенциальных конкурентах в деятельности предприятия, оценке качества деловых отношений с конкурирующими предприятиями в различных сферах деловой активности.

9. Сведения о подготовке, проведении и результатах переговоров с деловыми партнерами предприятия.

10. Сведения об условиях конфиденциальности, из которых можно установить порядок соглашения и другие обязательства предприятия с партнерами (клиентами, контрагентами).

11. Сведения о методах расчета, структуре, уровне реальных цен на продукцию и размеры скидок.

12. Сведения о подготовке к участию в торгах и аукционах, результатах приобретения или продажи на них товаров.

13. Сведения о целях, задачах, программах перспективных научных исследований. Ключевые идеи научных разработок, точные значения конструкционных характеристик, создаваемых изделий и оптимальных параметров разрабатываемых технологических процессов (размеры, объемы, конфигурация, процентное содержание компонентов, температура, давление, время и т.д.). Аналитические и графические зависимости, отражающие найденные закономерности и взаимосвязи, данные об условиях экспериментов и оборудовании, на котором они проводились. Сведения о материалах, из которых изготовлены отдельные детали, об особенностях конструкторско-технологического, художественно-технического решения изделия, дающие положительный экономический эффект.

Сведения о методах защиты от подделки товарных и фирменных знаков, о состоянии парка ПЭВМ и программного обеспечения.

14. Сведения об особенностях используемых и разрабатываемых технологий и специфике их применения, об условиях их производства и транспортировке продукции.

15. Сведения о порядке и состоянии организации защиты коммерческой тайны, о порядке и состоянии организации охраны, системы сигнализации, пропускном режиме.

Сведения, составляющие коммерческую тайну предприятия, предприятий-партнеров и передаваемые ими в пользование на доверительной основе, и другие сведения.

5. ОРГАНИЗАЦИЯ ДОПУСКА И ДОСТУПА ПЕРСОНАЛА К КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

5.1. Основные положения допуска персонала предприятия к конфиденциальной информации

В соответствии со статьей 6 Федерального закона РФ "Об информации, информационных технологиях и защите информации" вопросы ограничения доступа к информации, определения порядка и условий такого доступа отнесены к компетенции обладателя информации.

Обладатель информации при осуществлении своих прав обязан ограничивать доступ к информации и принимать меры по ее защите, если такая обязанность установлена федеральными законами.

В настоящее время в нашем государстве законодательно урегулированы (определены) и подробно раскрыты вопросы допуска и доступа должностных лиц и граждан к сведениям, составляющим государственную или коммерческую тайну. Порядок допуска лиц к иным видам информации с ограниченным доступом с учетом положений Федерального закона РФ "Об информации, информационных технологиях и защите информации" находится в компетенции соответствующих должностных лиц (обладателей такой информации).

Доступ граждан к сведениям (информации), в установленном порядке отнесенным к коммерческой тайне, осуществляется в соответствии со статьями 7 и 10 Федерального закона РФ "О коммерческой тайне".

С момента установления в отношении информации, составляющей коммерческую тайну, режима коммерческой тайны, полномочия по принятию решения о доступе к ней, переходят к обладателю информации.

Необходимо отметить, что определение порядка доступа лиц к коммерческой тайне и учет лиц, получивших такой допуск, являются одними из мер по охране конфиденциальности такой информации, принятие которых для обладателя информации в соответствии с Федеральным законом РФ "О коммерческой тайне" является обязательным.

Меры по охране конфиденциальности информации признаются разумно достаточными, если исключается доступ к информации, составляющей коммерческую тайну, любых лиц без согласия ее обладателя.

Иные, не противоречащие законодательству России меры по ограничению порядка доступа к коммерческой тайне, могут быть дополнительно приняты ее обладателем.

Одним из вопросов государственного регулирования в сфере защиты государственной тайны является порядок допуска и доступа должностных лиц и граждан к сведениям, составляющим государственную тайну. Эта область является наиболее значимой для решения задач по защите государственной тайны и, в связи с этим, будет в данном учебном пособии раскрыта подробнее.

Допуск и непосредственный доступ должностных лиц и граждан к сведениям, составляющим государственную тайну, и их носителям, осуществляется в соответствии с положениями Закона РФ "О государственной тайне" на основа-

нии "Инструкции о порядке допуска должностных лиц и граждан Российской Федерации к государственной тайне"[34].

Допуск граждан к государственной тайне осуществляется соответствующими руководителями органов государственной власти, предприятий и организаций.

Допуск граждан к государственной тайне осуществляется в добровольном порядке и предусматривает:

- принятие на себя допущенными к государственной тайне лицами обязательств перед государством по нераспространению доверенных им сведений, составляющих государственную тайну;

- согласие на частичные временные ограничения их прав в соответствии с Законом РФ "О государственной тайне";

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

- определение видов, размеров и порядка предоставления льгот, предусмотренных законодательством Российской Федерации;

- ознакомление с нормами законодательства Российской Федерации о государственной тайне, предусматривающими ответственность за их нарушение;

- принятие соответствующего решения руководителем предприятия о допуске оформляемого лица к государственной тайне.

Должностное лицо или гражданин, допущенные (ранее допускавшиеся) к государственной тайне, могут быть временно ограничены в следующих своих правах:

- в праве на выезд за границу на срок, оговоренный в трудовом договоре (контракте) при оформлении допуска гражданина к государственной тайне;

- в праве на распространение сведений, составляющих государственную тайну, и на использование открытий и изобретений, содержащих такие сведения;

- в праве на неприкосновенность частной жизни при проведении проверочных мероприятий в период оформления допуска к государственной тайне.

Ограничение гражданина в праве на выезд из Российской Федерации осуществляется в соответствии с Федеральным законом РФ "О порядке выезда из Российской Федерации и въезда в Российскую Федерацию"[35].

В целях частичной компенсации ограничений в правах для должностных лиц и граждан, допущенных к государственной тайне на постоянной основе, устанавливаются следующие льготы:

- 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 и организациями организационных и (или) штатных мероприятий.

Для сотрудников подразделений по защите государственной тайны дополнительно к вышеперечисленным льготам устанавливается процентная

---

[34] Утверждена постановлением Правительства РФ от 28.10.1995 г. № 1050 "Об утверждении Инструкции о порядке допуска должностных лиц и граждан Российской Федерации к государственной тайне".

[35] Федеральный закон РФ от 15.08.1996 г. № 114-ФЗ "О порядке выезда из Российской Федерации и въезда в Российскую Федерацию".

надбавка к заработной плате за стаж работы в указанных структурных подразделениях[36].

Граждане, которым по характеру занимаемой ими должности необходим доступ к государственной тайне, могут быть назначены на эти должности (приняты на работу) только после оформления в установленном порядке допуска по соответствующей форме.

Перечень должностей, при назначении на которые граждане обязаны оформлять допуск к сведениям, составляющим государственную тайну, в связи с возложением на них соответствующих должностных (функциональных) обязанностей, определяется номенклатурой должностей. Номенклатура должностей разрабатывается предприятием, согласовывается с соответствующим органом Федеральной службы безопасности Российской Федерации (далее - орган безопасности), и после этого согласования утверждается руководителем предприятия (его заместителем, возглавляющим работу по защите государственной тайны).

Изменения и дополнения в номенклатуру должностей вносятся в установленном порядке по мере необходимости. Полная переработка номенклатуры должностей осуществляется не реже одного раза в 5 лет.

Порядок разработки, согласования, утверждения номенклатуры, а также внесения в нее изменений и дополнений определяются "Инструкцией о порядке допуска должностных лиц и граждан Российской Федерации к государственной тайне".

С целью подтверждения фактической работы (ознакомления) сотрудников предприятия со сведениями, составляющими государственную тайну, подразделение по защите государственной тайны ведет учет их осведомленности в этих сведениях.

5.2. Порядок оформления и переоформления допуска к государственной тайне. Формы допуска

Допуск к государственной тайне - процедура оформления права граждан на доступ к сведениям, составляющим государственную тайну.

В соответствии со степенями секретности сведений, составляющих государственную тайну, и грифами секретности их носителей, установлены следующие формы допуска:

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.

Проверочные мероприятия, связанные с допуском граждан к государственной тайне, осуществляются соответствующими органами безопасности во взаимодействии с органами, осуществляющими в соответствии с законодательством оперативно-розыскную деятельность.

Уровень необходимого допуска личного состава определяется степенью секретности сведений (грифом секретности их носителей), с которыми они зна-

[36] Определено постановлением Правительства РФ от 18.09.2006 г. № 573 "О предоставлении социальных гарантий гражданам, допущенным к государственной тайне на постоянной основе, и сотрудникам структурных подразделений по защите государственной тайны".

комятся (работают) в рамках исполнения должностных обязанностей. Уровень допуска для каждого должностного лица, работающего на предприятии, отражается в Номенклатуре должностей.

Для непосредственного оформления допуска к государственной тайне лицам, принимаемым на работу на должности, включенные в Номенклатуру должностей, кадровый орган предприятия (лицо, ведущее кадровую работу) осуществляет подготовку необходимых материалов. Перечень таких материалов и соответствующие формы документов приведены в "Инструкции о порядке допуска должностных лиц и граждан Российской Федерации к государственной тайне".

Основным документом, отражающим анкетные, автобиографические и другие данные оформляемого лица, является анкета, собственноручно им заполняемая.

Основным учетным документом, содержащим отметки о согласовании допуска лица с органом безопасности, непосредственном решении руководителя предприятия о допуске лица к носителям сведений, составляющих государственную тайну, а также отражающим трудовую деятельность оформляемого лица, его семейное положение и другую информацию, является карточка о допуске. Форма карточки определяется в зависимости от формы допуска к государственной тайне, на которую оформлено данное лицо.

Направление вышеперечисленных, а также других необходимых документов в орган безопасности производится с мотивированным письмом, содержащим обоснование необходимости допуска лица к сведениям соответствующей степени секретности.

Согласование допуска к государственной тайне оформляется в карточке о допуске, которая возвращается на предприятие и хранится в структурном подразделении по защите государственной тайне.

Правовой основой взаимоотношений руководителя предприятия и допущенного к государственной тайне лица, является договор (контракт) об оформлении допуска к государственной тайне, являющийся приложением к трудовому договору, заключаемому в соответствии с разделом III Трудового кодекса РФ.

Данный договор (контракт) оформляется с учетом предусмотренных статьей 24 Закона РФ "О государственной тайне" для лиц, допущенных к государственной тайне, ограничений; в нем отражаются взаимные обязательства руководителя предприятия и работника. Заключение договора (контракта) до проведения проверочных мероприятий не допускается.

Хранение договоров (контрактов) о допуске к государственной тайне и соответствующих карточек о допуске осуществляется установленным порядком в структурном подразделении по защите государственной тайны предприятия.

Переоформление допуска лиц по первой и второй формам производится соответственно через 10 или 15 лет только в случае перехода указанных граждан на другое место работы. Переоформление допуска лиц, постоянно работающих на предприятии, оформившем им допуск, не производится.

Независимо от сроков действия переоформление допуска по первой или второй форме производится в случаях:

- перевода или приема гражданина на работу (назначения на должность) в подразделения по защите государственной тайны;

- вступления гражданина в брак за исключением особо оговоренных в нормативных документах случаях;

- возвращения из длительных сроком свыше 6 месяцев заграничных командировок;

- выезда близких родственников допущенного к государственной тайне лица за границу на постоянное место жительства;

- возникновения обстоятельств, являющихся в соответствии с Законом РФ "О государственной тайне" основаниями для отказа гражданину в допуске к государственной тайне.

Перечень направляемых в орган безопасности документов определен в "Инструкции о порядке допуска должностных лиц и граждан Российской Федерации к государственной тайне".

При несоответствии формы допуска лица степени секретности сведений, к которым он фактически имеет доступ, форма допуска должна быть изменена.

Снижение формы допуска с первой на вторую (третью) или со второй на третью оформляется распоряжением руководителя предприятия с соответствующей отметкой в карточке о допуске к государственной тайне. В случае производственной необходимости руководитель, ранее снизивший форму допуска работнику, может восстановить ее без проведения проверочных мероприятий органами безопасности.

Предприятие в необходимых случаях в установленном порядке обязано письменно информировать орган безопасности о состоянии работы по допуску лиц к государственной тайне (изменение формы допуска, прекращение допуска и т.д.) и предоставлять необходимые отчетные документы и материалы.

5.3. Основания для отказа должностному лицу или гражданину в допуске к государственной тайне и условия прекращения допуска

При оформлении допуска к государственной тайны в отношении оформляемого лица и его близких родственников в порядке, установленном законодательством Российской Федерации, уполномоченные органы проводят проверочные мероприятия. Объем проверочных мероприятий зависит от степени секретности сведений, к которым будет допускаться оформляемое лицо. Проверочные мероприятия осуществляются в соответствии с законодательством Российской Федерации.

Цель проведения проверочных мероприятий - выявление оснований, являющихся в соответствии с Законом РФ "О государственной тайне" основаниями для отказа гражданину в допуске к государственной тайне.

В соответствии со статьей 22 Закона РФ "О государственной тайне" такими основаниями могут являться:

- признание гражданина судом недееспособным, ограниченно дееспособным или особо опасным рецидивистом, нахождение его под судом или следствием за государственные или иные тяжкие преступления, наличие у него неснятой судимости за эти преступления;

- наличие у гражданина медицинских противопоказаний для работы с использованием сведений, составляющих государственную тайну, согласно перечню, утверждаемому в установленном порядке[37];

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

- выявление в результате проведения проверочных мероприятий действий оформляемого лица, создающих угрозу безопасности Российской Федерации;

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

Решение об отказе гражданину в допуске к государственной тайне принимается руководителем предприятия в индивидуальном порядке с учетом результатов проверочных мероприятий.

После оформления в установленном порядке должностному лицу или гражданину допуска к государственной тайне в процессе исполнения им своих должностных (функциональных) обязанностей в зависимости от сложившихся личных или иных других обстоятельств могут возникнуть условия, являющиеся препятствием наличию у него такого допуска.

В соответствии со статьей 23 Закона РФ "О государственной тайне" допуск гражданина к государственной тайне может быть прекращен в случае:

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

- однократного нарушения им предусмотренных трудовым договором (контрактом) обязательств, связанных с сохранением государственной тайны;

- возникновения обстоятельств, являющихся в соответствии с Законом РФ "О государственной тайне" основанием для отказа гражданину в допуске к государственной тайне.

Прекращение допуска к государственной тайне гражданину осуществляется по решению руководителя предприятия, в котором он работает. Это решение оформляется в виде письменного мотивированного заключения.

В случае, когда заключение о нецелесообразности дальнейшего допуска гражданина к сведениям, составляющим государственную тайну, вынесено органом безопасности, оно является обязательным основанием для отстранения этого гражданина от работы со сведениями, составляющими государственную тайну.

Решения руководителя предприятия об отказе гражданину в допуске к государственной тайне, о прекращении гражданину допуска и расторжении на основании этого трудового договора (контракта) с ним могут быть обжалованы в вышестоящий орган государственной власти (организацию) или в суд.

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

К сведениям, составляющим государственную тайну, без проведения проверочных мероприятий допускаются Члены Совета Федерации, депутаты Государственной Думы, судьи на период исполнения ими своих полномочий, а также

---

[37] Приказ Министерства Здравоохранения РФ от 16.03.1999 г. № 83 "О перечне медицинских противопоказаний для осуществления работы с использованием сведений, составляющих государственную тайну".

адвокаты, участвующие в качестве защитников в уголовном судопроизводстве по делам, связанным со сведениями, составляющими государственную тайну.

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 отбирается соответствующая расписка.

5.4. Организация доступа персонала предприятия к сведениям, составляющим государственную тайну

Доступ к сведениям, составляющим государственную тайну - санкционированное полномочным должностным лицом ознакомление конкретного лица со сведениями, составляющими государственную тайну.

Организация доступа должностного лица или гражданина к сведениям, составляющим государственную тайну, возлагается на руководителя соответствующего органа государственной власти, предприятия или организации, а также на их структурные подразделения по защите государственной тайны.

Руководитель предприятия обязан осуществлять постоянный контроль за соответствием формы допуска граждан степени секретности сведений, к которым они фактически имеют доступ.

Он несет персональную ответственность за создание таких условий, при которых должностное лицо или гражданин знакомятся только с теми сведениями, составляющими государственную тайну, и в таких объемах, которые необходимы ему для выполнения его должностных (функциональных) обязанностей.

Основанием для непосредственного доступа лица к сведениям, составляющим государственную тайну, и их носителям, является решение руководителя предприятия, оформляемое в карточке о допуске.

После принятия такого решения под руководством непосредственного руководителя (руководителя предприятия) гражданин изучает положения нормативно-методических документов, определяющих вопросы защиты государственной тайны в ходе выполнения им своих должностных (функциональных) обязанностей. Изучаются внутренние организационно-распорядительные документы предприятия, задачи и функции структурных подразделений в этой области.

Особое внимание должно быть уделено специфике деятельности предприятия, а также особенностям проведения работ с использованием сведений, составляющих государственную тайну.

В необходимых случаях планируются и с привлечением структурных подразделений по защите государственной тайны проводятся занятия с лицами, допущенными к государственной тайне.

Завершающим этапом подготовки к непосредственному выполнению обязанностей по занимаемой должности, связанных с использованием и защитой сведений, составляющих государственную тайну, является сдача зачетов по знанию нормативно-методических документов и особенностей решения данных задач на предприятии.

Прием зачетов осуществляет комиссия, состоящая, как правило, из сотрудников подразделений по защите государственной тайны, представителей профилирующих подразделений, а также подразделения, на должность в которое назначен данный сотрудник.

Результаты зачета оформляются в форме акта, который хранится в структурном подразделении по защите государственной тайны.

В дальнейшем основные положения вышеупомянутых нормативно-методических документов, обязанности и права лиц, допущенных к сведениям, составляющим государственную тайну, ежегодно (с принятием зачетов) доводятся до всех сотрудников, работающих на предприятии и имеющих допуск к государственной тайне.

5.5. Порядок доступа к конфиденциальной информации командированных лиц

Доступ командированных лиц к коммерческой тайне на предприятиях, куда они командируются по служебным вопросам, осуществляется в порядке, определяемом обладателем информации, составляющей коммерческую тайну в соответствии с установленным режимом коммерческой тайны. Порядок доступа лиц к конфиденциальной информации иного характера в каждом конкретном случае устанавливается ее обладателем, наделенном соответствующими полномочиями.

Доступ командированных лиц к сведениям, составляющим государственную тайну, осуществляется в соответствии с положениями нормативных документов по защите государственной тайны.

Основаниями для доступа командированного лица к сведениям, составляющим государственную тайну, и их носителям, являются следующие документы:

- паспорт или иной документ, удостоверяющий личность командированного лица;
- справка о допуске по соответствующей форме, подтверждающая наличие у командированного лица права на ознакомление (работу) со сведениями соответствующей степени секретности;
- предписание на выполнение задания.

Справка о допуске и предписание на выполнение задания оформляются порядком, определенным в "Инструкции о порядке допуска должностных лиц и граждан Российской Федерации к государственной тайне".

Справка о допуске подписывается руководителем подразделения по защите государственной тайны или кадрового органа и заверяется печатью предприятия, в котором постоянно работает командированное лицо.

Предписание на выполнение задания подписывается руководителем предприятия или соответствующего структурного подразделения предприятия, заверяется печатью предприятия и выдается для посещения только одной организации. В нем кратко указывается основание командирования и определяется, с какими сведениями, составляющими государственную тайну, необходимо ознакомить командируемое лицо для выполнения им служебного задания.

В случае, когда в предписании необходимо отразить сведения, составляющие государственную тайну, оно пересылается почтой в порядке, установленном для секретных документов.

Командированное лицо может иметь доступ только к тем сведениям, составляющим государственную тайну (их носителям), которые ему необходимы в рамках выполняемого задания, указанного в предписании на выполнение задания.

Непосредственный доступ командированного лица к конкретным сведениям (их носителям) осуществляется с письменного разрешения руководителя принимающего предприятия, либо руководителя структурного подразделения предприятия, которое оформляется в соответствующей графе предписания на выполнение задания.

Указанное разрешение служит основанием для ознакомления (работы) командированного лица с конкретными носителями сведений, составляющих государственную тайну (секретными документами и материалами). Выдача этих носителей командированному лицу для ознакомления (работы) осуществляется порядком, определенным нормативными документами по защите государственной тайны.

По завершении командирования лица на предприятие, его доступа и ознакомления (работы) со сведениями, составляющими государственную тайну, производится оформление документов командированного лица.

В предписании на выполнении задания, которое остается на предприятии, куда командировалось лицо, руководителем предприятия или соответствующего структурного подразделения производится отметка о степени секретности сведений, с которыми фактически ознакомилось командированное лицо. Отметка подтверждается подписью командированного лица, после чего предписание передается для хранения в подразделение по защите государственной тайны предприятия.

В справке о допуске указываются степень секретности сведений, с которыми ознакомилось командированное лицо, и дата. Запись заверяется подписью руководителя подразделения по защите государственной тайны предприятия и печатью предприятия. По возвращении из командировки справка о допуске командированным лицом сдается на хранение в подразделение по защите государственной тайны предприятия, в которой постоянно работает это лицо.

Руководитель организации и подразделение по защите государственной тайны должны принимать все необходимые меры к созданию таких условий для приема командированных лиц, при которых исключалась бы возможность их несанкционированного ознакомления со сведениями, составляющими государственную тайну, не предусмотренными целями и задачами командировки и не указанными в предписании на выполнение задания.

6. ОСНОВНЫЕ НАПРАВЛЕНИЯ И МЕТОДЫ РАБОТЫ С ПЕРСОНАЛОМ ПРЕДПРИЯТИЯ, ДОПУЩЕННЫМ К КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

Персонал предприятия, допущенный в силу должностных (функциональных) обязанностей к сведениям конфиденциального характера, - основной субъект правоотношений в сфере защиты конфиденциальной информации. Одновременно он является и единственным ее "нематериальным носителем".

В решении проблемы комплексной защиты информации на предприятии все более значительное место занимает выбор эффективных способов и методов работы с персоналом предприятия. Персонал предприятия, являясь генератором новых идей, открытий и изобретений, ускоряющих научно-технический прогресс, направляет максимальные усилия на повышение благосостояния предприятия в целом и каждого его сотрудника в частности.

Руководство решает задачу сохранения в тайне сотрудниками предприятия путей, методов и способов повышения благосостояния предприятия и достижения максимальной прибыли в его работе.

Однако, несмотря на это, персонал предприятия, являясь основным "носителем" конфиденциальной информации, становится и основным источником ее возможной утечки (разглашения).

В настоящее время от того, насколько сотрудник предприятия подготовлен профессионально в области защиты информации, какими он обладает морально-деловыми и психологическими качествами, всецело зависит его способность противостоять возможным попыткам получения злоумышленниками или представителями организаций-конкурентов важной для них информации, в силу этого отнесенной данным предприятием к категории конфиденциальной.

Высокий уровень подготовки сотрудников предприятия в вопросах защиты конфиденциальной информации позволит также максимально снизить вероятность появления непреднамеренных ошибок в обращении с этой информацией (ее носителями), наличие которых также потенциально создает предпосылки к ее получению (завладению) вышеуказанными "недоброжелателями".

И наоборот, проявление сотрудниками предприятия своих низких профессиональных навыков и отрицательных морально-деловых качеств значительно снизит эффективность системы защиты конфиденциальной информации на предприятии в целом, так как никакие меры организационного и технического характера не скомпенсируют возможную утечку информации со стороны сотрудников предприятия, являющихся ее основными "носителями".

К основным факторам и обстоятельствам, чаще всего приводящим к разглашению конфиденциальной информации персоналом предприятия, к ней допущенным, относятся:

- недостаточный уровень знаний положений нормативных актов и внутренних организационно-распорядительных документов предприятия по организации и обеспечению защиты информации;

- слабый контроль со стороны руководителей всех уровней за состоянием защиты информации и эффективностью принимаемых мер по недопущению утечки этой информации;

- недостаточное внимание вопросам организации работы с персоналом предприятия, изучению морально-деловых качеств сотрудников предприятия, допущенных к конфиденциальной информации;

- несвоевременное принятие эффективных и действенных мер по предотвращению разглашения персоналом предприятия конфиденциальной информации, а также по фактам нарушения норм и правил защиты информации сотрудниками предприятия, и другие.

Вопросы охраны конфиденциальности информации, к которой допускается работник предприятия, закреплены в разделе III Трудового кодекса РФ.

В соответствии с его положениями в заключаемом работодателем с работником трудовом договоре могут предусматриваться условия о неразглашении работником охраняемой законом тайны (государственной, служебной, коммерческой и иной).

Трудовой договор, заключенный с работником предприятия, может быть расторгнут работодателем в случае однократного грубого нарушения работником трудовых обязанностей - разглашения охраняемой законом тайны (государ-

ственной, коммерческой, служебной и иной), ставшей известной работнику в связи с исполнением им трудовых обязанностей.

С учетом изложенного постоянная работа с персоналом предприятия, имеющим доступ к конфиденциальной информации, сегодня является одним из наиболее актуальных и важных направлений деятельности руководства и должностных лиц предприятия.

Эта работа на предприятии должна организовываться и проводиться в плановом порядке, на постоянной основе. Неотъемлемой частью этой работы является распределение руководством предприятия задач и функций между должностными лицами и соответствующими структурными подразделениями. Определяются приоритетность и очередность выполнения этих функций и задач.

Самое непосредственное участие в работе с персоналом предприятия, как правило, принимают: кадровый орган, подразделение по защите государственной тайны, подразделение воспитательной работы, юридическая служба (юрисконсульт), служба охраны и служба собственной безопасности.

Работа с сотрудниками предприятия, независимо от степени конфиденциальности информации, к которой они допущены (допускались или будут допускаться), проводится в несколько этапов:

- при приеме кандидата на работу, связанную с доступом к конфиденциальной информации (перевод на эту работу штатного сотрудника предприятия);
- в ходе выполнения сотрудником предприятия, допущенным к конфиденциальной информации, должностных (функциональных) обязанностей;
- непосредственно перед увольнением и в процессе увольнения сотрудника с предприятия (переводе на должность, не связанную с доступом к конфиденциальной информации).

Усилия руководства предприятия в этой работе должны быть сосредоточены на следующих основных направлениях:

- изучение морально-деловых качеств сотрудников предприятия;
- повышение ответственности сотрудников всех категорий за сохранность в тайне доверенных по службе сведений конфиденциального характера;
- проведение профилактической работы по предупреждению (исключению) утечки конфиденциальной информации путем ее разглашения;
- повышение уровня теоретических знаний и практических навыков сотрудников в вопросах защиты конфиденциальной информации;
- создание и поддержание устойчивого морально-психологического климата в коллективе предприятия;
- создание и применение системы стимулирования труда сотрудников, допущенных к конфиденциальной информации.

В работе с персоналом предприятия, допущенным к конфиденциальной информации, используются следующие методы:

- обучения;
- инструктажей;
- индивидуальной и воспитательной работы;
- проверки уровня знаний;
- контроля.

Метод обучения - первостепенный метод работы с персоналом предприятия, начальный этап в приобретении теоретических знаний и практических навыков обеспечения защиты конфиденциальной информации в рамках выпол-

нения должностных (функциональных) обязанностей по основной специальности.

Процесс обучения сотрудников предприятия должен быть постоянным и планомерным, так как система защиты конфиденциальной информации предприятия требует развития и совершенствования.

Метод инструктажей применяется руководством предприятия и руководителями структурных подразделений с целью доведения до сотрудников, работающих с конфиденциальной информацией, положений вновь принятых (утвержденных) нормативно-методических документов, а также требований вышестоящих органов государственной власти (предприятий).

Во время инструктажей особое внимание должно уделяться анализу практической работы на предприятии по исключению возможных каналов утечки сведений конфиденциального характера и возникающих угроз защите информации.

Метод индивидуальной и воспитательной работы заключается в систематическом и целенаправленном воздействии на процесс формирования и развития личности сотрудника предприятия в целях наиболее полного использования его профессиональных возможностей и способностей, деловых, высоких моральных и иных положительных качеств в интересах обеспечения сохранности доверенных по службе (работе) сведений конфиденциального характера.

Цель проверки уровня знаний - проверить и оценить степень подготовленности каждого сотрудника предприятия к выполнению практических задач по защите информации на основе знаний положений нормативно-методических и внутренних организационно-распорядительных документов. Проверка уровня знаний проводится как руководством предприятия, так и сотрудниками структурных подразделений по защите государственной тайны, служб безопасности, подразделений охраны.

Метод контроля в работе с персоналом предприятия имеет своей целью оценку эффективности работы каждого сотрудника предприятия по организации и обеспечению защиты конфиденциальной информации, использованию при этом всех имеющихся сил и средств предприятия. Контроль может быть периодическим (плановым) и внезапным. Проводится сотрудниками штатных подразделений предприятия, решающих задачи по организации защиты информации.

Вышеперечисленные направления и методы работы с персоналом характерны для предприятий, осуществляющих работу с использованием сведений конфиденциального характера независимо от вида и степени конфиденциальности информации.

Наиболее полно вышеизложенные вопросы определены в Федеральном законе РФ "О коммерческой тайне", который установил правовые основы организации и проведения работы с персоналом предприятия, допущенным к коммерческой тайне.

Этим федеральным законом закреплен принцип добровольности доступа к коммерческой тайне работника предприятия (если иное не предусматривается трудовым договором).

Установлены функции работодателя по отношению к сотруднику предприятия в целях охраны конфиденциальности информации, составляющей коммерческую тайну.

Работодатель обязан:

- ознакомить под расписку работника, доступ которого к информации, составляющей коммерческую тайну, необходим для выполнения им своих трудовых обязанностей, с перечнем информации, составляющей коммерческую тайну, обладателями которой являются работодатель и его контрагенты;

- ознакомить под расписку работника с установленным работодателем режимом коммерческой тайны и с мерами ответственности за его нарушение;

- создать работнику необходимые условия для соблюдения им установленного работодателем режима коммерческой тайны.

Особенности работы с персоналом предприятия, допущенным в установленном порядке к сведениям, составляющим государственную тайну, определены в "Инструкции о порядке допуска должностных лиц и граждан Российской Федерации к государственной тайне".

В этой работе особое внимание уделено этапу приема и оформления на работу гражданина на должность, связанную с допуском к государственной тайне. В этой связи конкретизированы функции, возлагаемые на кадровый орган предприятия (должностное лицо, ведущее кадровую работу) и его работника, ответственного за работу с кандидатами при их приеме на работу.

Так, в ходе предварительной беседы с оформляемым на работу гражданином работник кадрового органа наряду с уточнением отдельных вопросов анкеты, заполняемой при оформлении материалов на допуск к государственной тайне, выявляет представляющие интерес сведения, не предусмотренные вопросами анкеты:

- выясняет у гражданина, имел ли он за последний год отношение к секретным работам, документам и изделиям;

- давал ли он обязательство по неразглашению сведений, составляющих государственную тайну;

- работал ли (служил) на режимных объектах.

Работник кадрового органа также запрашивает необходимые справки и документы, знакомит гражданина с содержанием договора (контракта) об оформлении допуска к государственной тайне.

В дополнение к вышеперечисленным направлениям и методам работы с персоналом предприятия, допущенным к конфиденциальной информации, руководитель предприятия, непосредственно отвечающий за организацию защиты информации, вправе принять не противоречащие законодательству дополнительные меры по исключению утечки (разглашения) сотрудниками своего предприятия охраняемых сведений.

7. ОРГАНИЗАЦИЯ ВНУТРИОБЪЕКТОВОГО И ПРОПУСКНОГО РЕЖИМОВ НА ПРЕДПРИЯТИИ

7.1. Роль и место внутриобъектового и пропускного режимов в общей системе защиты информации на предприятии

Внутриобъектовый и пропускной режимы устанавливаются на предприятиях, осуществляющих в предусмотренном законодательством Российской Федерации порядке работу со сведениями, составляющими государственную тайну.

Внутриобъектовый и пропускной режимы являются основными элементами системы защиты информации предприятия.

Их организация является обязательным условием соблюдения требований нормативно-методических документов по защите государственной (коммерческую) тайны, предоставляющим предприятию право на проведение в установленном порядке работ, связанных с использованием сведений, составляющих государственную (коммерческую) тайну.

Основными общими целями организации внутриобъектового и пропускного режимов на предприятии являются исключение (предотвращение):

- проникновения посторонних лиц на охраняемую (режимную) территорию и объекты предприятия, а также в служебные помещения, в которых проводятся работы с использованием сведений, составляющих государственную (коммерческую) тайну;

- посещения режимных помещений без служебной необходимости сотрудниками предприятия, не имеющими к ним прямого отношения, а также командированными лицами, не имеющими служебного задания на их посещение (работу в них);

- вноса (ввоза) на территорию предприятия личных технических средств: кино-, фото-, видео-, звукозаписывающей аппаратуры и других технических средств;

- несанкционированного выноса (вывоза) с территории предприятия носителей сведений, составляющих государственную (коммерческую) тайну;

- нарушений установленного регламента служебного времени, распорядка работы структурных подразделений по защите государственной (коммерческой) тайны, а также установленного порядка и режима работы сотрудников предприятия и командированных лиц с носителями сведений, составляющих государственную (коммерческую) тайну.

Организация и обеспечение внутриобъектового и пропускного режимов на предприятии в совокупности направлены на соблюдение всеми сотрудниками предприятия и командированными лицами надлежащего режима секретности.

Режим секретности - это установленный нормативными актами единый порядок обеспечения защиты сведений, составляющих государственную (коммерческую) тайну, включающий систему административно-правовых, организационных, инженерно-технических и других мер.

Таким образом, внутриобъектовый и пропускной режимы являются неотъемлемой частью системы установления и реализации комплекса мероприятий, направленных на защиту сведений, составляющих государственную (коммерческую) тайну, и сохранность их носителей.

В данном разделе учебного пособия будут раскрыты основные положения организации внутриобъектового и пропускного режимов на предприятии, их цели и задачи, а также задачи, возлагаемые на должностных лиц и сотрудников предприятий.

Более подробно вопросы организации внутриобъектового и пропускного режимов изложены в нормативно-методических документах, разрабатываемых федеральными органами исполнительной власти применительно к возложенным на них функциям и в соответствии с решаемыми ими задачами. Эти нормативно-методические документы раскрывают особенности формирования и функционирования систем защиты информации в органах государственной власти, на предприятиях и в организациях. В связи с их конкретной направленностью указанные нормативно-методические документы имеют ограничение на их распро-

странение и на доступ к их содержанию, однако они могут быть изучены и использованы в практической работе выпускниками образовательных учреждений после их назначения на предприятия на должности специалистов по защите информации.

7.2. Основные цели, подходы и принципы организации внутриобъектового режима

Внутриобъектовый режим - совокупность комплекса мероприятий, направленных на обеспечение установленного режима секретности непосредственно в структурных подразделениях, на объектах и в служебных помещениях предприятия.

Основными целями внутриобъектового режима на предприятии являются:

- определение требований по общему режиму секретности на предприятии на основе положений нормативных правовых актов и указаний вышестоящих органов государственной власти (предприятий);
- ограничение круга лиц, допускаемых к сведениям, составляющим государственную (коммерческую) тайну, и их носителям;
- регламентация порядка и правил непосредственной работы сотрудников предприятия, а также командированных лиц, с носителями сведений, составляющих государственную (коммерческую) тайну;
- планирование комплекса мероприятий, направленных на исключение утечки сведений, составляющих государственную (коммерческую) тайну, и утрат носителей этих сведений;
- организация контроля со стороны должностных лиц предприятия и структурных подразделений по защите государственной (коммерческой) тайны за выполнением требований по режиму секретности на предприятии;
- организация работы с персоналом предприятия, допущенным к сведениям, составляющим государственную (коммерческую) тайну, а также с вновь принимаемыми на работу гражданами.

Задачи по организации внутриобъектового режима на предприятии возлагаются, как правило, на заместителя руководителя предприятия, отвечающего за вопросы защиты государственной (коммерческой) тайны. Заместитель руководителя предприятия работу по формированию внутриобъектового режима организует на основе всестороннего анализа возможных каналов утечки сведений, составляющих государственную (коммерческую) тайну, при проведении предприятием всех видов работ.

В ходе выполнения этой работы руководством предприятия используются следующие основные подходы к организации внутриобъектового режима:

- определение ответственности руководителей подразделений и должностных лиц;
- четкое разграничение функций, возлагаемых на структурные подразделения по защите государственной (коммерческой) тайны (режимно-секретный орган, подразделение противодействия иностранным техническим разведкам, служба охраны и др.);
- создание эффективной системы контроля выполнения мероприятий по режиму секретности и сохранностью носителей сведений, составляющих государственную (коммерческую) тайну.

При формировании системы внутриобъектового режима руководитель предприятия и соответствующие должностные лица должны обеспечить реализацию следующих основных принципов:

- принципа персональной ответственности руководителей структурных подразделений, других должностных лиц и сотрудников предприятия за выполнение задач в интересах защиты государственной (коммерческой) тайны;
- принципа комплексного использования имеющихся сил и средств для решения задач по защите государственной (коммерческой) тайны;
- принципа полного охвата всех направлений деятельности предприятия, в ходе которых возможна утечка сведений, составляющих государственную (коммерческую) тайну, или утрата носителей этих сведений.

Внутриобъектовый режим предусматривает планирование и выполнение на предприятии следующих основных мероприятий:

- выявление возможных каналов утечки сведений, составляющих государственную (коммерческую) тайну, и реализация мер, направленных на их закрытие;
- лицензирование и сертификация деятельности в области защиты информации;
- отнесение сведений к государственной (коммерческой) тайне, засекречивание и рассекречивание сведений и их носителей;
- подбор, изучение и оформление лиц для назначения на должности, предусматривающие оформление допуска к государственной (коммерческой) тайне;
- индивидуальная и воспитательная работа с персоналом предприятия, допущенным к государственной (коммерческой) тайне;
- распределение обязанностей между должностными лицами и сотрудниками предприятия в области защиты государственной (коммерческой) тайны;
- допуск и непосредственный доступ сотрудников предприятия к сведениям, составляющим государственную (коммерческую) тайну (их носителям); ограничение круга лиц, допускаемых к данным сведениям;
- учет, хранение, уничтожение носителей сведений, составляющих государственную (коммерческую) тайну, установление режима и порядка работы сотрудников предприятия с этими носителями сведений;
- противодействие техническим средствам разведки конкурента и защита информации от несанкционированного доступа при использовании средств автоматизации;
- организация подготовки, переподготовки и повышения квалификации сотрудников предприятия, допущенных к государственной (коммерческой) тайне;
- организация и проведение совещаний, в ходе которых обсуждаются вопросы, содержащие сведения, составляющие государственную (коммерческую) тайну;
- защита государственной (коммерческой) тайны в ходе осуществления предприятием международного сотрудничества с иностранными государствами (организациями);
- защита государственной (коммерческой) тайны при выполнении научно-исследовательских, опытно-конструкторских работ и других видов совместных

работ, связанных с передачей сведений, составляющих государственную (коммерческую) тайну, другим предприятиям и организациям;

- финансовое, материально-техническое и другие виды обеспечения защиты государственной тайны;

- исключение утечки сведений, составляющих государственную (коммерческую) тайну в ходе издательской и рекламной деятельности предприятия;

- оборудование помещений, в которых проводятся работы с использованием сведений, составляющих государственную (коммерческую) тайну, или хранятся носители этих сведений;

- контроль эффективности решения задач по защите государственной (коммерческой) тайны должностными лицами и структурными подразделениями предприятия;

- контроль наличия носителей сведений, составляющих государственную (коммерческую) тайну.

7.3. Силы и средства, используемые при организации внутриобъектового режима

Важнейшую роль в организации внутриобъектового режима выполняют руководитель предприятия и его заместитель, в соответствии со своими должностными обязанностями непосредственно возглавляющий работу по защите государственной (коммерческой) тайны.

В соответствии с нормативными актами непосредственная ответственность за организацию и осуществление необходимых мероприятий по защите государственной (коммерческой) тайны возлагается на руководителя предприятия.

Руководитель предприятия, с учетом анализа состояния защиты государственной (коммерческой) тайны и результатов контроля эффективности решения задач по защите государственной (коммерческой) тайны должностными лицами и структурными подразделениями предприятия, определяет (уточняет) задачи этим должностным лицам и структурным подразделениям. Он обязан:

- предъявлять высокую требовательность к должностным лицам и сотрудникам предприятия, принимать меры по недопущению разглашения сведений, составляющих государственную (коммерческую) тайну, утрат носителей сведений, строго взыскивать с сотрудников предприятия, допускающих факты безответственности и халатности в работе со сведениями, составляющими государственную (коммерческую) тайну;

- оценивать деятельность сотрудников предприятия по вопросам защиты государственной (коммерческой) тайны;

- направлять работу должностных лиц и сотрудников предприятия на строгое соблюдение требований режима секретности.

Заместитель руководителя предприятия отвечает за практическую деятельность структурных подразделений предприятия и должностных лиц по защите государственной (коммерческой) тайны. В интересах организации внутриобъектового режима он выполняет следующие основные функции:

- осуществляет разработку организационно-планирующих документов предприятия по защите государственной (коммерческой) тайны, организует контроль за их исполнением;

- максимально ограничивает круг должностных лиц, допускаемых к сведениям, составляющим государственную (коммерческую) тайну;

- лично возглавляет работу на предприятии по защите государственной (коммерческую) тайны;

- организует проведение систематического анализа деятельности структурных подразделений и должностных лиц предприятия, направленной на обеспечение защиты государственной (коммерческой) тайны;

- организует и поддерживает строгий порядок в разработке, обращении, учете, хранении и уничтожении носителей сведений, составляющих государственную (коммерческую) тайну;

- организовывает защиту информации при использовании средств автоматизации;

- организует подбор, расстановку и обучение сотрудников структурных подразделений по защите государственной (коммерческой) тайны;

- обеспечивает необходимые условия для правильной организации режима секретности, учета, хранения, уничтожения носителей сведений, составляющих государственную (коммерческую) тайну, и обращения с ними;

- принимает меры по защите государственной (коммерческой) тайны при осуществлении предприятием международного сотрудничества, взаимодействии с иностранными партнерами;

- лично инструктирует работу комиссий предприятия по проверке наличия носителей сведений, составляющих государственную (коммерческую) тайну, отбору и уничтожению носителей, утративших актуальность и практическое значение, а также не требующихся в работе.

При организации внутриобъектового режима используется совокупность имеющихся на предприятии структурных подразделений по защите государственной (коммерческой) тайны, а также других подразделений, решающих задачи в интересах защиты государственной (коммерческой) тайны, и применяемых этими подразделениями средств защиты информации.

Необходимо обратить внимание, на то, что в соответствии со статьей 6 Федерального закона РФ "Об оперативно-розыскной деятельности"[38] приобретение и использование специальных технических средств, предназначенных для негласного получения информации, службой безопасности предприятия подлежит лицензированию в органах Федеральной службы безопасности РФ. В случае нарушения правил приобретения специальных технических средств, предназначенных для негласного получения информации, а также их незаконное использование в охранной деятельности руководители предприятия и сотрудники службы безопасности подвергаются административному наказанию по статьям 20.23 и 20.24 (соответственно) Кодекса РФ об административных правонарушениях (см. приложение 10).

Основными структурными подразделениями предприятия, участвующими в организации внутриобъектового режима, являются: режимно-секретное подразделение, служба безопасности предприятия, подразделение противодействия техническим средствам разведки конкурента[39], подразделение охраны (в части вопросов контроля внутренних объектов и служебных помещений предприятия).

---

[38] Федеральный закон РФ от 12.08.1995 г. № 144-ФЗ "Об оперативно-розыскной деятельности".

[39] Задачи, решаемые подразделением противодействия техническим средствам разведки конкурента, в данном учебном пособии рассматриваться не будут.

Функции, возложенные на подразделение охраны предприятия, в полном объеме будут изложены в соответствующей главе данного учебного пособия.

Основным структурным подразделением, участвующим в организации внутриобъектового режима на предприятии, а также осуществляющим контроль эффективности проводимых в этих целях мероприятий, является режимно-секретное подразделение.

Режимно-секретное подразделение выполняет следующие основные задачи:

- разработка совместно с другими подразделениями предприятия мероприятий по организации внутриобъектового режима;
- подготовка предложений руководству предприятия по ограничению круга лиц, допускаемых к конкретным сведениям, составляющим государственную (коммерческую) тайну, и их носителям;
- организация и ведение учета, обеспечение хранения, своевременное уничтожение носителей сведений, составляющих государственную (коммерческую) тайну;
- осуществление контроля порядка обращения с носителями сведений, составляющих государственную (коммерческую) тайну, сотрудниками предприятия;
- участие в выработке мер по исключению утечки сведений, составляющих государственную (коммерческую) тайну, при осуществлении предприятием связей с иностранными предприятиями и организациями;
- осуществление комплексного анализа состояния работы на предприятии по защите государственной (коммерческой) тайны, эффективности принимаемых должностными лицами и структурными подразделениями мер;
- участие в разработке развернутых перечней сведений, подлежащих засекречиванию, в работе экспертных комиссий по рассекречиванию сведений и их носителей;
- непосредственное участие в оформлении допуска к государственной (коммерческой) тайне сотрудникам предприятия, разработка номенклатуры должностей предприятия, подлежащих оформлению на допуск к сведениям, составляющим государственную (коммерческую) тайну.

Наряду с режимно-секретным подразделением важное место в организации внутриобъектового режима на предприятии занимает служба безопасности.

Служба безопасности создается решением руководителя на предприятиях, выполняющих работы одновременно с несколькими видами конфиденциальной информации, в том числе и со сведениями, составляющими государственную тайну.

В этом случае режимно-секретное подразделение предприятия может структурно входить в состав службы безопасности, и задачи, им решаемые, возлагаются также на службу безопасности.

Ниже будут рассмотрены общие задачи, решаемые службой безопасности при наличии в структуре предприятия самостоятельного режимно-секретного подразделения.

Службой безопасности предприятия в интересах организации внутриобъектового режима выполняются следующие основные задачи:

- обеспечение экономической безопасности, охраны собственности предприятия;

- организация конфиденциального делопроизводства, учета, хранения и уничтожения документов (материалов), содержащих конфиденциальную информацию;

- защита конфиденциальной информации при осуществлении внешнеэкономической деятельности предприятия;

- контроль выполнения требований нормативно-методических и внутренних организационно-распорядительных документов предприятия по обеспечению защиты охраняемой информации;

- выявление и закрытие возможных каналов утечки конфиденциальной информации;

- разработка системы организационных и технических мер, регламентирующих внутриобъектовый режим предприятия, организация и контроль их выполнения;

- осуществление контроля порядка изготовления, учета, хранения, использования бланков служебных удостоверений, печатей, штампов предприятия, а также металлических и мастичных печатей с индивидуальными учетными номерами;

- организация приема и передачи информации и открытой корреспонденции с использованием различных технических средств связи (телетайп, телефакс, электронная почта и т.п.);

- разработка требований к служебным помещениям, в которых проводятся работы с охраняемой информацией, а также хранятся носители этой информации, проведение их аттестации, организация установки и эксплуатации технических средств защиты этой информации;

- участие в экспертизе материалов, предназначенных для открытого опубликования;

- организация и проведение служебных расследований по фактам нарушений требований по защите охраняемой информации, а также внутриобъектового режима на предприятии;

- осуществление взаимодействия с правоохранительными и другими государственными органами по вопросам обеспечения безопасности предприятия.

Вышеперечисленные подразделения предприятия, решающие задачи по организации внутриобъектового режима в своей деятельности используют различные средства защиты информации.

Необходимо отметить важную роль организационных средств защиты информации в решении задач внутриобъектового режима.

Под организационными средствами защиты информации понимается комплекс организационно-технических мероприятий различного характера, планируемых и осуществляемых в интересах организации внутриобъектового режима.

Отличительной особенностью организационных средств защиты информации является их ярко выраженная организационная основа. Важность и необходимость применения организационных средств защиты информации заключается в их особом значении, так как они являются по своей сути связующим звеном между персоналом предприятия и различными техническими и иными средствами, используемыми в интересах организации и обеспечения режима секретности.

Наиболее эффективными мерами по защите информации, относящимися к организационным средствам защиты информации, являются:

- организация разработки, внедрения и использования различных средств и систем защиты информации;

- организация разработки, размножения, учета и уничтожения носителей конфиденциальной информации с использованием технических средств;

- контроль соблюдения персоналом предприятия установленных требований при использовании объектов информатизации;

- анализ эффективности функционирования технических систем и средств защиты информации;

- разработка и внедрение в практику инструкций и иных документов, регламентирующих порядок и правила обращения с конфиденциальной информацией.

Порядок организации внутриобъектового режима, задачи, решаемые должностными лицами и структурными подразделениями предприятия, отражаются в разрабатываемых на предприятии внутренних организационно-распорядительных документах, утверждаемых руководителем предприятия.

7.4. Цели и задачи пропускного режима

Пропускной режим - это совокупность норм и правил, регламентирующих порядок входа (выхода) лиц, въезда (выезда) транспортных средств на территорию предприятия, вноса (выноса), ввоза (вывоза) носителей сведений конфиденциального характера, а также мероприятий по реализации этих норм и правил с использованием имеющихся сил и средств.

Сущность пропускного режима заключается в объединении усилий, а также сил и средств, в интересах достижения основной цели организации пропускного режима - исключения несанкционированного (бесконтрольного) пребывания на территории предприятия посторонних лиц и (или) транспорта.

Под посторонними лицами или транспортом понимаются граждане или автомобильный и другой транспорт, не имеющие права (даже разового) посещения территории предприятия или пребывания на ней.

Основными задачами пропускного режима являются:

- недопущение проникновения посторонних лиц на территорию (объекты) или в служебные помещения предприятия;

- исключение посещения служебных помещений предприятия без служебной необходимости сотрудниками предприятия и командированными лицами;

- предотвращение вноса (ввоза) на территорию предприятия личных технических средств: кино-, фото-, видео-, звукозаписывающей аппаратуры и других технических средств;

- исключение несанкционированного выноса (вывоза) с территории предприятия носителей сведений конфиденциального характера;

- предотвращение хищения носителей сведений конфиденциального характера.

При организации пропускного режима на предприятии необходимо руководствоваться следующими основными принципами:

- централизация системы управления пропускным режимом;

- комплексный подход к использованию сил и средств в интересах решения задач пропускного режима;

- максимальное использование элементов автоматизации;

- оперативное реагирование и принятие решения в чрезвычайных ситуациях.

При организации пропускного режима на предприятии используются следующие основные термины и понятия:

охраняемая территория - это территория предприятия (включающая его объекты и служебные помещения), на которой установлен и реализуется комплекс мероприятий пропускного и внутриобъектового режимов;

территория с особым режимом пропуска - это территория предприятия (с расположенными на ней объектами и служебными помещениями), на которой устанавливаются дополнительные меры по обеспечению внутриобъектового и пропускного режимов;

пропуск - оформленный в установленном порядке именной документ, подтверждающий право законного пребывания должностного лица или гражданина на территории предприятия (ее объектах или в служебных помещениях).

7.5. Основные элементы системы организации пропускного режима, используемые силы и средства

В целях выполнения задач пропускного режима на территорию и объекты, а также в служебные помещения, на предприятиях создается система организации пропускного режима, в рамках которой обеспечивается комплексное применение имеющихся сил и средств.

Основными элементами системы являются:

- структурное подразделение по защите государственной (коммерческой) тайны (режимно-секретное подразделение);
- служба безопасности предприятия;
- бюро пропусков;
- контрольно-пропускные пункты.

Структурное подразделение по защите государственной (коммерческой) тайны (режимно-секретное подразделение) и служба безопасности предприятия[40] организуют выполнение комплекса мероприятий по пропускному режиму и осуществляют постоянный контроль эффективности их реализации.

Бюро пропусков создается для непосредственного решения задач по учету, хранению, уничтожению и выдаче всех видов пропусков сотрудникам предприятия, командированным и другим лицам, имеющим на это право.

На бюро пропусков возлагаются следующие основные задачи:

- учет, хранение всех видов пропусков, печатей, штампов, в том числе используемых для простановки условных знаков (шифров);
- оформление, выдача, замена и уничтожение пропусков;
- обеспечение контрольно-пропускных пунктов образцами действующих пропусков;
- проведение проверок наличия бланков всех видов пропусков;
- контроль за работой контрольно-пропускных пунктов.

В бюро пропусков находится список лиц, имеющих право подписи заявок на выдачу разовых пропусков, с образцами их подписей. Бюро пропусков на основании заявок на выдачу постоянных и временных пропусков, подписанных должностными лицами, определенными распоряжением руководителя предпри-

[40] Могут объединяться в одно структурное подразделение.

ятия (его заместителя), оформляет постоянные и временные пропуска. В заявках указываются: кому, по какому образцу, на какой срок и в какие структурные подразделения (на объекты, в служебные помещения) необходимо выдать пропуска.

На предприятиях, где штатными расписаниями бюро пропусков не предусмотрены, приказами руководителя предприятия назначаются сотрудники предприятия, на которых возлагается выполнение функций, возложенных на бюро пропусков. При работе в бюро пропусков двух и более сотрудников между ними распределяются должностные обязанности, которые утверждаются руководителем предприятия, его заместителем по режиму (безопасности) или начальником службы безопасности предприятия.

Контрольно-пропускные пункты служат для непосредственного осуществления пропускного режима на территорию и объекты предприятия в соответствии с установленным порядком его организации.

Контрольно-пропускные пункты решают следующие задачи:

- непосредственный контроль входа (выхода) лиц с территории (объектов) предприятия;
- учет въезда (выезда) транспорта на территорию предприятия;
- контроль законности выноса (вывоза) с территории предприятия носителей сведений конфиденциального характера;
- контроль своевременности возврата посетителями предприятия разовых пропусков;
- оперативное реагирование в нештатных ситуациях, связанных с попытками проникновения посторонних лиц (транспорта) на территорию (объекты) предприятия;
- взаимодействие с караулом (подразделениями охраны) при решении задач обеспечения пропускного режима.

Для несения службы на контрольно-пропускных пунктах назначаются наиболее дисциплинированные сотрудники службы охраны, способные обеспечить качественное выполнение задач контрольно-пропускной службы. Необходимо отметить, что осуществление частной охранной деятельности без специального разрешения (лицензии)[41] влечет административную ответственность по статье 20.16 Кодекса РФ об административных правонарушениях (см. приложение 10).

Сотрудники, несущие службу на контрольно-пропускных пунктах, обязаны проявлять бдительность, твердо знать образцы действующих пропусков всех видов и проставляемые на них условные знаки (шифры). При проверке предъявляемых пропусков они обязаны брать их в руки, особое внимание, при этом обращая на соответствие фотографии - личности предъявителя пропуска.

При проверке пропусков без фотографий (временных и разовых) лица, несущие службу на контрольно-пропускных пунктах, обязаны производить сверку пропусков с документами, удостоверяющими личность.

Контрольно-пропускные пункты оборудуются должным образом, особое внимание уделяется размещению в помещениях контрольно-пропускных пунктов необходимой документации. В витринах под стеклом на контрольно-пропускном пункте должны находиться:

[41] Порядок получения лицензии определен в статье 6 Закона РФ от 11.03.1992 г. № 2487-I "О частной детективной и охранной деятельности в Российской Федерации".

- выписка из инструкции по организации пропускного режима на предприятии;

- инструкции личному составу, несущему дежурство, в том числе по их действиям в случае пожара, стихийного бедствия и чрезвычайных ситуациях;

- образцы действующих пропусков всех видов;

- списки должностных лиц, которым предоставлено право подписи всех видов пропусков с образцами их подписей;

- номера телефонов для связи с соответствующими оперативными службами (местных и городских автоматических телефонных станций) и другая необходимая информация.

Основным средством обеспечения установленного пропускного режима являются вводимые в установленном порядке и действующие в течение определенного срока действия пропуска на территорию и объекты предприятия, в том числе используемые с условными знаками (шифрами).

При организации пропускного режима используются следующие виды пропусков:

постоянные - выдаются штатному персоналу предприятия;

временные - выдаются командированным на предприятие лицам - сотрудникам других организаций, а также вновь принятым на работу сотрудникам предприятия до оформления им постоянных пропусков;

разовые - выдаются на одно посещение посетителям предприятия посетителям и действуют в течение рабочего дня;

материальные - выдаются сотрудникам предприятия и предназначены для вноса (выноса), ввоза (вывоза) имущества (изделий) и других предметов.

Право подписи всех видов пропусков устанавливается решением руководителя предприятия и определяется соответствующим приказом.

Должностным лицам, которым в силу выполнения ими должностных обязанностей, необходимо круглосуточное посещение всех объектов (служебных помещений) предприятия, выдаются соответствующие пропуска (проставляются необходимые отметки). Круг таких лиц строго ограничивается руководителем предприятия или его заместителем по режиму (безопасности).

Для ограничения входа на отдельные объекты (в служебные помещения) предприятия на пропусках проставляются условные знаки (шифры).

Кроме того, на предприятии распоряжением руководителя предприятия определяется перечень сотрудников предприятия, которым в силу выполнения ими должностных обязанностей предоставляется право прохода через контрольно-пропускные пункты с рабочими папками (портфелями, рабочими чемоданами), предназначенными для переноски служебных документов (материалов). О предоставлении сотрудникам такого права указывается в их пропусках путем проставления в них соответствующих условных знаков (шифров).

На предприятиях, выполняющих работы с наиболее важными сведениями, составляющими государственную тайну, могут выделяться территории с особым режимом пропуска. Право прохода на эти территории предоставляется сотрудникам предприятия, имеющим непосредственное отношение к проводимым на них работам.

Для прохода (допуска) сотрудников предприятия на территории с особым режимом пропуска им выдаются специальные пропуска. В отдельных случаях

для этих целей могут использоваться условные знаки (шифры), проставляемые на постоянных пропусках вышеуказанных лиц.

Бланки всех видов пропусков учитываются и хранятся порядком, установленным для бланков строгой отчетности. Они выдаются сотрудникам предприятия (иным лицам) в соответствии с подписанными заявками и хранятся ими как служебные документы. При убытии в отпуск (командировку, на длительное лечение) пропуска передаются на временное хранение своему непосредственному начальнику (в бюро пропусков). При увольнении сотрудников предприятия пропуска у них отбираются.

Проверки наличия бланков всех видов пропусков осуществляются представителями службы безопасности (структурного подразделения по защите государственной тайны) и бюро пропусков предприятия в составе специально назначаемых для этих целей комиссий.

При утрате (хищении) или использовании пропуска посторонними лицами, при обезличенном пользовании пропуском, для изучения причин и обстоятельств данного факта, а также определения виновных лиц назначается и проводится служебное расследование. Результаты служебного расследования с анализом и выводами, включая меры ответственности к лицам, нарушившим установленные требования по организации пропускного режима, объявляются в приказе руководителя предприятия.

Изготовление бланков пропусков осуществляется предприятиями и учреждениями, имеющими соответствующие лицензии.

Образцы пропусков, проставляемые на них условные знаки (шифры), период времени, в течение которого они действуют, должностные лица, которым предоставляется право подписи всех видов пропусков, объявляются приказом руководителя предприятия.

Въезд (выезд) на территорию предприятия транспортных средств осуществляется по пропускам, выдаваемым их водителям, или по спискам, выданным на контрольно-пропускные пункты. В этих списках указываются: фамилии водителей, типы (марки) транспортных средств и их государственные регистрационные номера. Эти списки утверждаются заместителем руководителя предприятия по режиму (безопасности) или уполномоченными руководителями структурных подразделений предприятия. Личность водителей транспортных средств, указанных в списках, проверяется по документам, удостоверяющим его личность.

С целью исключения возможности проникновения посторонних лиц на территорию (объекты) предприятия, осуществляющего работу с конфиденциальной информацией, а также утечки защищаемой информации, разрабатывается "Инструкция по организации пропускного режима".

В данной инструкции определяются: порядок организации и обеспечения пропускного режима; порядок и регламент работы бюро пропусков и контрольно-пропускных пунктов, обязанности должностных лиц и порядок их действий в различных ситуациях. Инструкция утверждается руководителем предприятия, доводится до всех сотрудников предприятия (в части касающейся) и является одним из основных внутренних организационно-распорядительных документов.

8. ОРГАНИЗАЦИЯ ОХРАНЫ ПРЕДПРИЯТИЙ

Организация охраны является составной частью общей системы защиты конфиденциальной информации предприятия.

Вопросы организации и обеспечения надежной охраны территории предприятия и его объектов неразрывно связаны с системой организации пропускного режима на предприятии. Силы и средства, участвующие в решении задач охраны предприятий, являются составными элементами системы охраны предприятия.

От организации и эффективности функционирования системы охраны в полной мере зависит уровень и возможность решения задач пропускного и внутриобъектового режимов, так как их цели во многом совпадают. Системы пропускного и внутриобъектового режимов являются после системы охраны так называемыми последующими рубежами безопасности, предотвращающими доступ злоумышленника к охраняемой предприятием информации.

Главными целями охраны предприятия являются:

- предотвращение попыток проникновения посторонних лиц (злоумышленников) на территорию (объекты) предприятия;

- своевременное обнаружение и задержание лиц, противоправно проникнувших (пытающихся проникнуть) на охраняемую территорию[42];

- обеспечение сохранности находящихся на охраняемой территории носителей конфиденциальной информации и материальных средств и исключение, таким образом, нанесения ущерба предприятию;

- предупреждение происшествий на охраняемом объекте и ликвидация их последствий.

Основные задачи охраны:

- контроль объекта и охраняемой территории, в том числе территории с особым режимом пропуска, с целью обнаружения и предотвращения попыток несанкционированного прохода (проникновения) на них посторонних лиц (злоумышленников);

- обеспечение конфиденциальности и сохранения в тайне факта проведения закрытых мероприятий на предприятии (его объектах), обсуждаемых или рассматриваемых на них вопросов;

- сопровождение и охрана носителей конфиденциальной информации, в том числе служебных документов предприятия, материальных ценностей и грузов при их транспортировке и перевозке (доставке);

- защита объекта и территорий с особым режимом пропуска от насильственных действий и вооруженных нападений, которые могут нанести ущерб предприятию;

- участие в обеспечении пропускного режима посетителей, транспортных средств и грузов на охраняемую территорию (объекты предприятия) с целью установления личности и учета посетителей, ввоза, вывоза носителей конфиденциальной информации, грузов, материальных ценностей, предотвращения их не-

[42] За нарушение пропускного режима охраняемого объекта предусмотрена административная ответственность по статье 20.17 Кодекса РФ об административных правонарушениях (см. приложение 10).

санкционированного перемещения, а также фиксации следов, скрытых и открытых попыток хищения иного имущества предприятия;

- систематический анализ эффективности системы охраны, принимаемых должностными лицами мер по охране объектов предприятия, сохранности носителей конфиденциальной информации, материальных ценностей и грузов, и выработка предложений по совершенствованию системы охраны.

Для реализации главных целей и основных задач охраны предприятия (его объектов) создается система охраны.

Система охраны предприятия - совокупность используемых в интересах охраны предприятия сил и средств, а также способов и методов охраны предприятия и его объектов.

Система охраны включает личный состав подразделений охраны (караулов), технические средства и системы охраны, места размещения личного состава, выполняющего задачи охраны, и используемых технических средств, а также методы охраны объектов. В качестве мест размещения личного состава охраны может быть использован один из основных элементов системы организации пропускного режима - контрольно-пропускные пункты.

Используемые при охране предприятий технические средства охраны делятся на средства обнаружения; средства обнаружения и ликвидации.

Основные средства обнаружения: пожарная и охранная сигнализация, "тревожное" оповещение, охранное телевидение, охранное освещение, аппаратура проверки почтовой корреспонденции, радиосвязь, прямая внутренняя связь, прямая телефонная связь с милицией.

Основные средства обнаружения и ликвидации: средства пожаротушения, средства индивидуальной защиты, газовые ловушки, автотранспорт, оружие, инженерно-технические средства.

С целью обеспечения охраны предприятий и их объектов создаются штатные подразделения охраны, которые организационно могут быть объединены в службу охраны. Служба охраны включает посты охраны, группы (подразделения) сотрудников охраны, группу охраны и сопровождения материальных ценностей и грузов, "тревожную" группу (группу быстрого реагирования), а также подразделения сторожевых собак (при необходимости).

Основными обязанностями сотрудников охраны являются:

- обеспечение защиты охраняемых объектов от противоправных посягательств (действий злоумышленников и нарушителей);

- осуществление мероприятий по предупреждению нарушений пропускного и внутриобъектового режимов, установленных на предприятии;

- пресечение преступлений и административных правонарушений на охраняемых объектах предприятия;

- осуществление поиска и задержания лиц, незаконно проникших на охраняемые объекты;

- участие в установленном порядке в осуществлении контроля за соблюдением противопожарного режима, тушении пожаров, а также в ликвидации последствий аварий, катастроф, стихийных бедствий и других чрезвычайных ситуаций на охраняемых объектах;

- участие в пределах компетенции в проведении мероприятий по обеспечению защиты сведений конфиденциального характера и сохранности носителей этих сведений;

- оказание в пределах своей компетенции содействия правоохранительным органам в решении возложенных на них задач.

При выполнении возложенных на сотрудников подразделений охраны задач в пределах охраняемых объектов они имеют право:

- требовать от работников, должностных лиц охраняемых объектов и других граждан соблюдения пропускного и внутриобъектового режимов;

- проверять у лиц документы, удостоверяющие их личность, и документы, дающие право на вход (выход), въезд (выезд) транспортных средств, а также внос (вынос) и ввоз (вывоз) имущества;

- производить досмотр транспортных средств при въезде (выезде) на охраняемые объекты и с охраняемых объектов;

- проверять условия хранения имущества на охраняемых объектах, состояние инженерно-технических средств охраны. При выявлении нарушений, создающих на охраняемых объектах угрозу возникновения пожаров, безопасности людей, а также условий, способствующих хищениям имущества, принимать меры по пресечению указанных нарушений и ликвидации данных условий;

- производить административное задержание и доставление в служебное помещение охраны или орган внутренних дел лиц, совершивших преступления или административные правонарушения на охраняемых объектах, а также производить личный досмотр, досмотр вещей, изъятие вещей и документов, являющихся орудием или непосредственным объектом правонарушения. Обеспечивать охрану места происшествия и сохранность указанных вещей и документов;

- беспрепятственно входить в помещения охраняемых объектов и осматривать их при преследовании лиц, незаконно проникших на охраняемые объекты, а также для задержания лиц, подозреваемых в совершении преступлений или административных правонарушений;

- использовать транспортные средства собственников охраняемых объектов для преследования лиц, совершивших преступления или административные правонарушения на охраняемых объектах, и доставления их в орган внутренних дел;

- в случаях и порядке, установленном законодательством Российской Федерации, применять физическую силу, специальные средства и огнестрельное оружие.

На предприятиях, входящих в структуру федеральных органов исполнительной власти, с целью защиты охраняемых объектов, являющихся государственной собственностью и находящихся в сфере ведения данных органов, в соответствии с Федеральным законом РФ "О ведомственной охране"[43] создаются и функционируют подразделения ведомственной охраны.

Главным требованием, предъявляемым к системе охраны, является ее надежность. Надежность охраны предприятия и его объектов достигается эффективным применением сил и средств охраны, правильной организацией и бдительным несением службы сотрудниками охраны (личным составом караулов) на постах охраны (контрольно-пропускных пунктах).

Выбор конкретных сил и средств, применяемых для охраны объекта предприятия, осуществляется на основе анализа возможных угроз его безопасности. Немаловажное значение, при этом, имеет уровень подготовки и профессиона-

[43] Федеральный закон РФ от 14.04.1999 г. № 77-ФЗ "О ведомственной охране".

лизм сотрудников охраны, осуществляющих непосредственное выполнение своих функций в местах несения дежурства.

Опыт показывает, что наибольшее количество нарушений системы охраны объектов обусловлено следующими основными причинами:

- недооценка возможных угроз безопасности объекта на конкретных рубежах (территориях) охраны;

- некачественное (халатное) исполнение обязанностей сотрудниками охраны при несении дежурства;

- использование нарушителем (злоумышленником) случайной (нештатной) ситуации. При этом частным случаем данной ситуации может быть преднамеренное создание персоналом службы охраны условий, способствующих таким злоумышленным действиям.

Таким образом, анализ возможных угроз безопасности охраняемого объекта, реальная оценка возможностей по созданию эффективной системы охраны с учетом возможного выбора имеющихся сил и средств и принятие на основе этого обоснованного и правильного решения, являются основой создания надежной системы охраны предприятия.

Организация системы охраны предприятия и его объектов устанавливаются решением руководителя предприятия. Подготовку такого решения осуществляют структурные подразделения, отвечающие за защиту конфиденциальной информации и безопасность предприятия.

При организации системы охраны определяются (устанавливаются):

- способы охраны территории предприятия и его объектов;

- количество постов, мест несения дежурства по охране объектов, участки (зоны, территории) охраны;

- количество и виды контрольно-пропускных пунктов, порядок и особенности несения дежурства на этих пунктах сотрудниками охраны;

- порядок и особенности действий личного состава охраны во всех случаях (в том числе в экстренных ситуациях);

- порядок и особенности применения (использования) технических средств обнаружения и охраны на каждом участке (зоне, территории) охраны.

Охрана предприятия может осуществляться как силами и средствами создаваемых в структуре предприятия подразделений охраны (службы охраны), так и путем использования услуг частных охранных предприятий, имеющих право в соответствии с законодательством осуществлять этот данный вид деятельности. Порядок оказания такими предприятиями услуг в сфере охраны, права и обязанности сотрудников частных охранных предприятий при выполнении ими задач охраны объектов определены Законом РФ "О частной детективной и охранной деятельности в Российской Федерации"[44].

Одними из способов охраны объектов предприятия являются: использование технических средств охраны (сигнализации), оконечные устройства которых выведены на пульты централизованного наблюдения в подразделения вневедомственной охраны при органах внутренних дел, а также несение дежурства работниками вневедомственной охраны непосредственно на объекте охраны.

[44] Закон РФ от 11.03.1992 г. № 2487-1. "О частной детективной и охранной деятельности в Российской Федерации".

Функции, возлагаемые на подразделения вневедомственной охраны, и порядок их деятельности определяются "Положением о вневедомственной охране при органах внутренних дел Российской Федерации"[45].

С целью определения задач, основных направлений охраны, используемых для осуществления охраны сил, средств, способов и методов на предприятии разрабатывается инструкция по организации охраны предприятия, его территории и объектов.

В данной инструкции определяются также порядок и особенности несения дежурства (выполнения задач) подразделениями охраны, порядок действий личного состава подразделения охраны в различных ситуациях и другие вопросы. Инструкция утверждается руководителем предприятия, доводится под роспись до личного состава подразделения охраны, а также, в части касающейся, до всех сотрудников предприятия.

9. ОРГАНИЗАЦИЯ ЗАЩИТЫ ИНФОРМАЦИИ ПРИ ПРОВЕДЕНИИ СОВЕЩАНИЙ, В ХОДЕ ИЗДАТЕЛЬСКОЙ И РЕКЛАМНОЙ ДЕЯТЕЛЬНОСТИ

9.1. Планирование мероприятий по защите информации при подготовке к проведению совещания

В ходе повседневной деятельности предприятий, связанной с использованием сведений, составляющих государственную тайну, и конфиденциальной информации, планируются и проводятся служебные совещания[46], в ходе которых рассматриваются или обсуждаются вопросы, содержащие конфиденциальную информацию.

Это могут быть вопросы, отнесенные к государственной тайне, касающиеся проводимых предприятием научно-исследовательских, опытно-конструкторских и иных видов работ, предусмотренных уставом предприятия, или вопросы, носящие конфиденциальный характер, отражающие коммерческую сторону деятельности предприятия.

Вышеперечисленные мероприятия могут быть внутренними (к участию в них привлекается только персонал данного предприятия) или внешними (с участием представителей сторонних организаций-партнеров).

Решение на проведение совещания во всех случаях принимается непосредственно руководителем предприятия или его заместителем по ходатайству руководителя подразделения, в чьих интересах оно будет проведено.

Принимаемые должностными лицами предприятия (структурным подразделением, его организующим) меры по защите конфиденциальной информации в ходе подготовки и проведения совещания должны носить как организационный, так и технический характер.

Мероприятия по защите информации проводятся при подготовке, в ходе проведения и по окончании совещания.

---

[45] Утверждено постановлением Правительства РФ от 14.08.1992 г. № 589.

[46] В данной главе под совещаниями понимаются также переговоры и другие мероприятия, проводимые с участием представителей как предприятия-организатора, так и сторонних предприятий-участников.

Одним из важных элементов в работе руководства и должностных лиц предприятия по защите информации при проведении совещания является этап планирования конкретных организационно-технических мер, направленных на исключение утечки конфиденциальной информации и на ее защиту.

Планирование мероприятий по защите информации включает выработку конкретных мер, определение ответственных за их реализацию должностных лиц (структурных подразделений) предприятия и сроков их выполнения (проведения).

Планирование мероприятий по защите информации, проводимых в ходе совещания с участием представителей сторонних организаций, осуществляется под руководством руководителя предприятия и при непосредственном участии его заместителя, возглавляющего на предприятии работу по защите информации. При отсутствии в структуре предприятия данного должностного лица, непосредственная ответственность за проведение планирования мероприятий по защите информации возлагается на руководителя режимно-секретного подразделения (службы безопасности).

Проведение совещания без приглашения представителей сторонних организаций может проводиться без участия режимно-секретного подразделения (службы безопасности). В этих случаях ответственность за планирование и проведение мероприятий по исключению утечки конфиденциальной информации и по ее защите возлагаются на руководителя структурного подразделения предприятия, организующего данное совещание.

При планировании совещания предусматривается такая очередность рассмотрения вопросов, при которой будет исключено участие в их обсуждении лиц, не имеющих к ним прямого отношения.

Непосредственная разработка плана подготовки и проведения совещания возлагается на структурное подразделение предприятия, организующее его проведение. В этом подразделении назначается должностное лицо, отвечающее за его подготовку, согласование с другими заинтересованными подразделениями предприятия, режимно-секретным подразделением (службой безопасности) и представление в установленном порядке на утверждение руководителю предприятия (его заместителю). После утверждения плана руководством предприятия он доводится в части касающейся до всех заинтересованных должностных лиц (руководителей подразделений), до лиц, назначенных ответственными за выполнение отдельных мероприятий плана, он доводится под роспись.

Подготовка плана осуществляется заблаговременно до начала совещания и включает мероприятия, проводимые перед проведением совещания, во время проведения совещания и по его завершении.

В плане указываются время и место проведения совещания, состав участников, перечень предприятий, участвующих в совещании.

План мероприятий по защите информации при подготовке и в ходе проведения совещания содержит следующие основные разделы:

1. Определение состава участников и их оповещение. В разделе отражаются: порядок формирования списка лиц, привлекаемых к участию в совещании, а также перечня предприятий, которым необходимо направить запросы с приглашениями; порядок подготовки и направления таких запросов; формирование содержания запросов.

2. Подготовка служебных помещений, в которых планируется проведение совещания. В разделе отражаются: работа по выбору служебных помещений; проверка соответствия помещений требованиям по защите информации; необходимость и целесообразность принятия дополнительных организационно-технических мер, направленных на исключение утечки информации; оборудование рабочих мест участников совещания, в том числе средствами автоматизации, на которых разрешена обработка конфиденциальной информации. Определяется порядок использования средств звукоусиления, кино- и видеоаппаратуры (проекторов).

3. Определение объема обсуждаемой информации. В данном разделе отражаются: порядок определения перечня вопросов, выносимых на совещание, и очередности их рассмотрения; порядок оценки степени конфиденциальности вопросов; выделение вопросов, к которым допускается узкий круг лиц, участвующих в совещании.

4. Организация пропускного режима на территорию и в служебные помещения, в которых проводится совещание. В разделе отражаются вопросы организации и осуществления пропускного режима: виды пропусков и проставляемых на них условных знаком (шифров) для прохода в конкретные служебные помещения; порядок учета, хранения, выдачи и выведения их из действия (сроки уничтожения); режим прохода, посещения и пребывания в помещениях участников совещания. Определяются количество и регламент работы основных и дополнительных контрольно-пропускных пунктов для прохода участников совещания на территорию и в служебные помещения.

5. Организация допуска участников совещания к рассматриваемым вопросам. Раздел содержит мероприятия, касающиеся непосредственного допуска участников к вопросам, выносимым на совещание, с учетом порядка их обсуждения и степени конфиденциальности информации, к которой допущен каждый участник совещания.

6. Осуществление записи (стенограммы), фото-, кино-, видеосъемки совещания. В разделе определяются порядок и возможные способы записи, съемки (стенографирования) хода совещания и обсуждаемых вопросов с учетом их конфиденциальности, а также должностные лица (подразделения), отвечающие за техническое обеспечение данного процесса.

7. Меры по защите информации непосредственно при проведении совещания. В разделе отражаются: порядок и способы охраны служебных помещений, меры по исключению прохода (проникновения) в них посторонних лиц, а также участников совещания, не участвующих в рассмотрении конкретных вопросов; мероприятия по предотвращению утечки информации по техническим каналам, силы и средства, задействованные при их проведении. Также определяются конкретные меры, исключающие визуальный просмотр и прослушивание ведущихся переговоров и обсуждения вопросов участниками совещания.

8. Организация учета, хранения, выдачи и рассылки материалов совещания. В разделе отражаются порядок учета, хранения, размножения (печатания, ксерокопирования), выдачи, рассылки и уничтожения материалов совещания, а также рабочих тетрадей (блокнотов), предназначенных для записи обсуждаемых вопросов участниками совещания. Определяется порядок обращения с данными носителями информации непосредственно в ходе совещания и после его окончания. Особое внимание уделяется порядку учета, хранения, размножения и ис-

пользования материалов совещания, зафиксированных на магнитных носителях (исполненных в электронном виде).

9. Оформление документов лиц, принимавших участие в совещании. В данном разделе отражается порядок и сроки оформления документов, подтверждающих право доступа участников совещания к конфиденциальной информации, предписаний (доверенностей) на участие в совещании, командировочных удостоверений;

10. Проверка и обследование места проведения совещания после его окончания. Раздел содержит мероприятия по организации и проведению визуальной проверки, а также проверки с использованием специальных технических средств (аппаратуры) помещений, в которых проводилось совещание с целью выявления оставленных (забытых) технических устройств, носителей конфиденциальной информации и личных вещей участников совещания.

11. Организация контроля выполнения требований по защите информации. В разделе отражается порядок, способы и методы контроля полноты и качества проводимых мероприятий, направленных на предотвращение утечки сведений конфиденциального характера, разглашения информации, содержащей такие сведения, и утрат (хищений) носителей информации. Указываются структурные подразделения (должностные лица), на которые возлагаются вопросы контроля.

Определяется система и порядок представления ответственными должностными лицами докладов о наличии носителей конфиденциальной информации и выявленных нарушениях в работе по защите конфиденциальной информации.

Для каждого включаемого в план мероприятия определяются: срок (время) его проведения и ответственное за выполнение мероприятия должностное лицо (подразделение).

9.2. Организация допуска участников совещания к обсуждаемым вопросам. Подготовка места проведения совещания

При использовании в ходе совещания сведений конфиденциального характера или обсуждении вопросов, содержащих такие сведения, руководство предприятия-организатора, осуществляет комплекс мероприятий, направленных на исключение ознакомления с ней посторонних лиц и сотрудников фирм-конкурентов.

На совещание приглашаются работники, имеющие непосредственное отношением к рассматриваемым (обсуждаемым) вопросам.

При обсуждении в ходе совещания вопросов, содержащих сведения, составляющие государственную тайну, его участники должны иметь допуск к этим сведениям по соответствующей форме, а при рассмотрении вопросов, отнесенных к иным видам конфиденциальной информации, в установленном порядке оформленное решение руководителя предприятия на допуск к данной категории (виду) информации.

При последовательном рассмотрении вопросов, имеющих различную степень конфиденциальности, к участию в совещании по каждому из рассматриваемых вопросов допускаются лица, имеющие к ним непосредственное отношение.

Должностное лицо, ответственное за проведение совещания, по указанию руководителя предприятия (подразделения, в чьих интересах проводится совещание) формирует список лиц, участвующих в совещании.

Этот список составляется на основании письменных обращений руководителей организаций, приглашенных к участию в совещании, и решений руководителей подразделений предприятия-организатора по привлечению к участию в совещании своих сотрудников.

В списке по каждому участнику указываются: фамилия, имя, отчество; наименование места работы и занимаемая должность; номер допуска к сведениям, составляющим государственную тайну, или номер решения руководителя о допуске к иной конфиденциальной информации; номера вопросов совещания, к обсуждению которых допущен участник. При необходимости в списке могут указываться и другие сведения.

Подготовленный список участников согласовывается с режимно-секретным подразделением (службой безопасности) предприятия-организатора совещания и утверждается руководителем этого предприятия, давшим разрешение на его проведение.

Включенные в список участники совещания проходят в служебные помещения, в которых проводится совещание, предъявляя службе охраны (службе безопасности) документ, удостоверяющий личность. Допускается проход в помещения участников совещания организовывать по пропускам, выдаваемым им исключительно на период проведения совещания и отличающимся от других используемых предприятием-организатором видов и образцов пропусков.

Проверку документов, подтверждающих наличие у участников совещания допуска к сведениям, составляющим государственную тайну, и разрешений на ознакомление с конфиденциальной информацией, осуществляет служба безопасности (режимно-секретное подразделение) предприятия-организатора совещания.

Участники совещания имеют право посещения только тех служебных помещений, в которых будут обсуждаться вопросы, к которым эти участники имеют непосредственное отношение.

Совещания проводятся в служебных помещениях, в которых в установленном порядке разрешено обсуждение вопросов конфиденциального характера, и приняты предусмотренные нормативными правовыми актами необходимые организационно-технические мероприятия, предотвращающие утечку защищаемой информации по техническим каналам.

В ходе проведения совещания разрешается использование фото-, кино-, видео- и звукозаписывающей аппаратуры, защита которой обеспечивается в соответствии с требованиями по противодействию иностранным техническим разведкам и технической защите информации.

Проверка служебных помещений на предмет возможности обсуждения в них вопросов конфиденциального характера проводится накануне совещания специально назначаемой комиссией, состоящей из специалистов по противодействию иностранным техническим разведкам и технической защите информации соответствующих подразделений предприятия-организатора.

9.3. Порядок проведения совещания и использования его материалов

Непосредственно перед началом совещания руководитель предприятия или должностное лицо, ответственное за его проведение, обязан проинформировать участников совещания о степени конфиденциальности обсуждаемых вопросов.

В ходе совещания, в том числе и во время перерывов, работник, ответственный за его проведение, совместно со службой безопасности (режимно-секретным подразделением) осуществляет необходимые организационно-технические мероприятия, направленные на исключение утечки сведений конфиденциального характера.

Во время перерывов в совещании, а также после завершения обсуждения одного вопроса и перехода к обсуждению следующего, сотрудники службы безопасности (службы охраны) организуют контроль прохода (нахождения) в служебные помещения, в которых проводится совещание, лиц в соответствии с утвержденным списком участников.

На все время проведения совещания запрещается пронос в служебные помещения, в которых оно проводится, индивидуальных видео- и звукозаписывающих устройств, а также средств связи (в том числе мобильных телефонов и приемников персонального вызова). В целях обеспечения их сохранности организуется камера хранения личных вещей участников совещания.

Звуко- и видеозапись, а также кино- и видеосъемка хода совещания и обсуждения вопросов совещания проводится с разрешения руководителя предприятия-организатора совещания только на учтенных в режимно-секретном подразделении (службе безопасности) носителях. При этом использование в этих целях соответствующей аппаратуры и технических устройств осуществляется при соблюдении требований по защите информации.

Носители конфиденциальной информации, а также сведений, составляющих государственную тайну, выдаются режимно-секретным подразделением (службой безопасности) участникам совещания под роспись, а после окончания совещания возвращаются. Контроль за своевременным возвратом этих носителей осуществляется сотрудниками вышеуказанных подразделений.

Для осуществления записей хода совещания и обсуждаемых вопросов участникам совещания установленным порядком выдаются рабочие тетради или рабочие блокноты, учтенные в службе безопасности (режимно-секретном подразделении) и имеющие соответствующий гриф секретности (степень конфиденциальности). Эти рабочие тетради (блокноты) по окончании совещания возвращаются в службу безопасности (режимно-секретное подразделение). При необходимости они могут быть секретной (конфиденциальной) почтой направлены для дальнейшего хранения и использования на предприятия, представители которых производили в них записи на совещании.

Итоговые документы совещания, а также материалы выступлений участников, в том числе и оформленные в электронном виде, в установленном порядке высылаются на предприятия, направлявшие на совещание своих представителей, а также в вышестоящие органы государственной власти (предприятия). Расчет рассылки материалов определяет руководитель предприятия-организатора.

Лицам, принимавшим участие в совещании, без письменного разрешения предприятия-организатора совещания запрещается использовать материалы совещания и его результаты при взаимодействии (проведении работ, переписке) с предприятиями, представители которых на него не приглашались.

9.4. Основы организации защиты информации в ходе издательской и рекламной деятельности предприятия

В настоящее время невозможно представить деятельность современного предприятия без его участия в издательской деятельности и рекламных акциях различного характера. Вместе с тем, для предприятий, осуществляющих работу с конфиденциальной информацией, такие его виды деятельности могут привести к распространению охраняемой информации о направлениях его деятельности и проводимых работах.

В связи с этим, в повседневной деятельности предприятия мероприятия по защите информации в процессе подготовки и реализации рекламных и издательских проектов занимают важное место.

В соответствии с Федеральным законом РФ "О рекламе"[47] в сфере рекламы используются следующие основные понятия:

реклама - информация, распространенная любым способом, в любой форме и с использованием любых средств, адресованная неопределенному кругу лиц и направленная на привлечение внимания к объекту рекламирования, формирование или поддержание интереса к нему и его продвижение на рынке;

объект рекламирования - товар, средство его индивидуализации, изготовитель или продавец товара, результаты интеллектуальной деятельности либо мероприятие (в том числе спортивное соревнование, концерт, конкурс, фестиваль, основанные на риске игры, пари), на привлечение внимания к которым направлена реклама;

товар - продукт деятельности (в том числе работа, услуга), предназначенный для продажи, обмена или иного введения в оборот;

рекламодатель - изготовитель или продавец товара либо иное определившее объект рекламирования и (или) содержание рекламы лицо;

рекламопроизводитель - лицо, осуществляющее полностью или частично приведение информации в готовую для распространения в виде рекламы форму;

рекламораспространитель - лицо, осуществляющее распространение рекламы любым способом, в любой форме и с использованием любых средств.

Основными видами осуществляемой предприятием рекламной деятельности с учетом положений федерального законодательства о рекламе, являются:

- наружная реклама, размещаемая на рекламных конструкциях в местах общего пользования. Под рекламными конструкциями в соответствии с Федеральным законом РФ "О рекламе" понимаются: щиты, стенды, строительные сетки, перетяжки, электронные табло и иные технические средства стабильного территориального размещения, монтируемые и располагаемые на внешних стенах, крышах и иных конструктивных элементах зданий, строений, сооружений или вне их, а также остановочных пунктов движения общественного транспорта;
- реклама на телевидении и радио, а также в периодических печатных изданиях;
- реклама, распространяемая по сетям электросвязи и размещаемая в почтовых отправлениях;
- реклама на транспортных средствах и с их использованием;

[47] Федеральный закон РФ от 13.03.2006 г. № 38-ФЗ "О рекламе".

- реклама в ходе проведения конференций, симпозиумов, организуемых и проводимых вне предприятия;

- реклама, размещаемая в глобальных информационных сетях общего пользования;

- реклама в ходе проведения внутренних мероприятий, проводимых предприятием с привлечением (приглашением, участием) представителей сторонних организаций и средств массовой информации.

Основными направлениями защиты конфиденциальной информации в ходе осуществления предприятием рекламной деятельности являются:

- подготовка и экспертиза предполагаемых к распространению рекламных материалов на предмет отсутствия в них информации с ограниченным доступом;

- анализ материалов, подготавливаемых рекламопроизводителем и рекламораспространителем к размещению в средствах рекламы;

- постоянный контроль порядка выхода и содержания рекламных материалов независимо от способа, формы и периодичности их распространения.

При принятии руководителем предприятия решения на рекламирование деятельности предприятия, а также производимых им товарах или услугах, должностное лицо, назначенное ответственным за подготовку рекламных материалов и их передачу рекламопроизводителю и (или) рекламораспространителю организует работу, направленную на предотвращение распространения в рекламе конфиденциальной информации. Комплекс мероприятий по защите информации включает проведение экспертизы предполагаемых к распространению материалов комиссией предприятия, анализ возможных форм, способов распространения рекламных материалов и непосредственное взаимодействие по вопросам организации и распространения материалов с рекламопроизводителем и рекламораспространителем.

Одним из важных элементов в этой работе является оценка комиссией предприятия, состоящей из компетентных специалистов, содержания материалов на предмет возможности их распространения, в том числе и объема этих материалов. После получения положительного заключения экспертной комиссии предприятия осуществляется подготовка договорных материалов на передачу рекламных материалов рекламопроизводителю и (или) рекламораспространителю, а также непосредственная передача материалов, предполагаемых к рекламному распространению.

В дальнейшем предприятие осуществляет постоянный контроль содержания рекламы при ее выходе в свет.

Государственный контроль в сфере рекламы осуществляет Федеральный антимонопольный орган и его территориальные органы.

Органы государственной власти, руководители предприятий, а также индивидуальные предприниматели и юридические лица (в том числе рекламопроизводители и рекламораспространители) обязаны представлять в антимонопольный орган информацию, необходимую для осуществления им полномочий по государственному контролю за соблюдением законодательства Российской Федерации о рекламе, и обеспечивать его уполномоченным должностным лицам доступ к такой информации.

Сведения, составляющие коммерческую, служебную и иную охраняемую законом тайну и полученные антимонопольным органом при осуществлении

своих полномочий, не подлежат разглашению, за исключением предусмотренных федеральным законом случаев.

В случае получения из вышеуказанных органов такого запроса руководитель предприятия организует предоставление в установленный срок запрашиваемой информации и направление органу, приславшему запрос, письменного уведомления о невозможности ее распространения без согласия предприятия-держателя информации.

В ходе повседневной деятельности предприятием с целью распространения информации о товарах (услугах) и проводимых предприятием работах могут осуществляться следующие виды издательской деятельности:

- в периодических печатных изданиях. Под периодическим печатным изданием понимаются: газета, журнал, альманах, бюллетень, иное издание, имеющее постоянное название, текущий номер и выходящее в свет не реже 1 раза в год;

- в глобальных информационных сетях;

- в однократно издаваемых сборниках, энциклопедиях, материалах конференций и т.п.;

- другими способами.

Усилия службы безопасности предприятия при проведении этих видов деятельности направляются на исключение утечки сведений, составляющих государственную тайну, и конфиденциальной информации. С этой целью на предприятии разрабатывается инструкция, определяющая задачи всех должностных лиц (структурных подразделений) предприятия в этой области.

Основными направлениями защиты информации при осуществлении предприятием издательской деятельности являются:

- определение тематики издаваемых материалов. Эта работа направлена на исключение из материалов тематик, содержащих конфиденциальную информацию и подготовку рекомендаций по исключению из них актуальной чувствительной информации, распространение которой может нанести ущерб предприятию;

- письменное согласование содержания материалов и возможности их издания с организациями-собственниками информации. Осуществляется ответственным за издание подразделением предприятия по согласованию со службой безопасности в форме письменного запроса в организации, являющиеся заказчиками или соисполнителями проводимых совместных и других работ, сведения о которых предполагается распространить;

- предварительная экспертиза материалов, предполагаемых к изданию, экспертной комиссией предприятия. Состав комиссии определяется приказом руководителя предприятия и включает представителей всех заинтересованных подразделений. В ходе работы комиссии проводится проверка материалов на предмет их издания с учетом возможных негативных последствий и нанесения возможного ущерба предприятию. По результатам работы комиссии подготавливаются заключение и рекомендации по частичному исключению из материалов актуальной информации (при необходимости);

- окончательная экспертиза подготовленных к изданию материалов, определение объема выпуска и способа их распространения.

После проведения вышеперечисленных мероприятий по завершении окончательной подготовки материалов к изданию службой безопасности пред-

приятия осуществляется контроль их печатания (тиражирования) непосредственно в типографии или иной организации (в зависимости от выбранного способа распространения).

9.5. Организация подготовки материалов к открытому опубликованию

С целью исключения распространения в средствах массовой информации сведений конфиденциального характера на предприятии планируется и проводится работа по анализу содержания материалов, предполагаемых к открытому распространению в средствах массовой информации.

Цель данной работы - недопущение утечки информации о деятельности предприятия, содержащей сведения с конфиденциального характера, а также сведений, составляющих государственную тайну, или служебную информацию ограниченного распространения (служебную тайну). Для достижения этой цели проводится комплекс организационных мероприятий. Планирование и осуществление данных мероприятий проводят: служба безопасности, структурное подразделение по защите государственной тайны или специально создаваемое в структуре предприятия подразделение (должностное лицо), на которое возлагаются вышеуказанные задачи.

Сотрудники предприятия, принимающие непосредственное участие в подготовке материалов к открытому опубликованию, должны знать и руководствоваться положениями статьи 5 Закона РФ "О государственной тайне", "Перечнем сведений, отнесенных к государственной тайне", другими нормативными актами, а также перечнем информации, составляющей коммерческую тайну предприятия.

Подготовка материалов к открытому опубликованию включает в себя их разработку авторами, предварительную проверку их содержания руководителями структурных подразделений предприятия, согласование возможности опубликования материалов со службой безопасности (подразделением по защите государственной тайны) предприятия.

Подготовленные к открытому опубликованию материалы не должны содержать сведений, составляющих государственную, коммерческую тайну, служебной информации ограниченного распространения (сведений, содержащих служебную тайну) и иной информации с ограниченным доступом, определенной нормативными правовыми актами.

Мероприятия, направленные на исключение открытого опубликования (распространения) информации с ограниченным доступом, включаются в план основных мероприятий по защите конфиденциальной информации предприятия на календарный год. В плане предусматриваются следующие основные мероприятия:

- разработка и утверждение руководителем предприятия организационно-распорядительных документов, определяющих порядок и особенности работы по подготовке материалов к открытому опубликованию;

- предварительный анализ и согласование материалов руководителями структурных подразделений предприятия, сотрудники которых осуществляют их подготовку к открытому опубликованию;

- анализ материалов, представляемых к открытому распространению, службой безопасности (подразделением по защите государственной тайны) предприятия;

- выборочный контроль изданных (опубликованных) материалов;

- проведение занятий с сотрудниками предприятия по доведению им положений нормативных правовых актов и внутренних организационно-распорядительных документов предприятия;

- взаимодействие с должностными лицами издательств (редакций) и средств массовой информации;

- определение состава экспертной комиссии предприятия по оценке возможности опубликования материалов и подготовка соответствующих заключений и осуществление ее деятельности;

- осуществление взаимодействия с другими предприятиями по вопросам открытого опубликования материалов, содержащих информацию о проводимых этими предприятиями совместных и других работах, а также с органами государственной власти и предприятиями, являющимися заказчиками работ и собственниками информации, предполагаемой к открытому опубликованию; получение письменного согласия этих органов государственной власти (предприятий) на открытое опубликование материалов;

- проведение периодического анализа эффективности проводимых мероприятий по исключению открытого опубликования сведений с ограниченным доступом и совершенствование этой работы на предприятии.

Ответственность за подготовку материалов к открытому опубликованию и соблюдение при этом требований по защите конфиденциальной информации несут авторы материалов, их непосредственные руководители (руководители соответствующих структурных подразделений) и руководитель предприятия.

Экспертиза материалов, предназначенных для открытого опубликования материалов, проводится с целью оценки их степени конфиденциальности и возможности открытого распространения (в отдельных случаях - при условии исключения из содержания материалов информации, распространение которой может нанести ущерб предприятию, или приведет к разглашению государственной тайны).

В обязательном порядке проводится экспертиза материалов, содержащих большой объем информации, а также материалов, тематика которых представляет широкий спектр вопросов, для изучения которых требуются специальные познания в различных сферах (областях науки, техники и профессиональной деятельности).

Для проведения экспертизы материалов, подготовленных к открытому опубликованию, приказом руководителя предприятия создается экспертная комиссия, как правило, сроком на один календарный год. В состав указанной комиссии назначаются сотрудники предприятия - специалисты в различных областях деятельности предприятия. Члены комиссии должны в необходимых случаях иметь допуск к государственной тайне, а также к иным видам конфиденциальной информации предприятия.

Сотрудники службы безопасности (подразделения по защите государственной тайны) в состав экспертной комиссии не включаются. В случае если лицо, являющееся членом экспертной комиссии, в конкретном случае является составителем, руководителем или редактором подготовленной к открытому опубликованию работы (материалов), то он не может принимать участия в работе экспертной комиссии по оценке этих материалов.

К проведению экспертизы по решению руководителя предприятия может быть привлечен руководитель структурного подразделения, в котором работает автор подготовленного материала.

К участию в работе экспертной комиссии могут быть привлечены представители других предприятий, имеющих отношение к рассматриваемым материалам (являющиеся собственниками информации, заказчиками проводимых работ и т.д.). Вопрос привлечения этих специалистов к работе в составе комиссии в каждом конкретном случае письменно согласовывается с соответствующими руководителями предприятий.

Руководитель предприятия-организатора экспертизы обязан создать членам экспертной комиссии условия, обеспечивающие рассмотрение материалов в соответствии с установленными требованиями, своевременно знакомить их с поступающими на предприятие нормативными актами и методическими документами по вопросам обеспечения защиты конфиденциальной информации, а также порядку (особенностям) проведения экспертизы.

Подготовку членов экспертной комиссии по вышеуказанным вопросам проводят сотрудники службы безопасности (подразделения по защите государственной тайны) предприятия или должностные лица, на которых данные вопросы возложены соответствующим приказом руководителя предприятия.

При подготовке и в ходе проведения экспертизы члены экспертной комиссии обязаны:

- знать перечни сведений, запрещенных к открытому опубликованию на предприятии, и строго руководствоваться ими при проведении экспертизы;

- при обнаружении в рассматриваемых материалах сведений, составляющих государственную, коммерческую или служебную тайну (служебную информацию ограниченного распространения), вынести заключение, запрещающее их открытое опубликование. Такие материалы передаются руководителю предприятия или его заместителю по безопасности (режиму) для принятия решения об их отнесении в установленном порядке к конфиденциальной информации соответствующего вида и об ограничении доступа к этой информации;

- проверять наличие письменного согласия руководителей предприятий - заказчиков работ (собственников информации) на опубликование материалов. Проверить выполнение рекомендаций (заключений) этих руководителей;

- рассматривать материалы с учетом ранее опубликованных работ, имеющих отношение к этим материалам, с тем, чтобы эта публикация не могла нанести ущерб безопасности предприятия или привести к разглашению сведений, составляющих государственную тайну;

- при рассмотрении сборников материалов (статей) принимать решение о возможности опубликования (издания) как всего сборника в целом, так и его отдельных статей (материалов).

Члены экспертной комиссии имеют право:

- получать от автора (авторов) письменное подтверждение об источниках, использованных им при подготовке материалов к опубликованию, а также другую информацию, необходимую для подготовки заключения;

- обращать в установленном порядке за соответствующей консультацией (разъяснениями) на другие предприятия, в органы государственной власти (к их должностным лицам).

Руководство работой комиссии осуществляет ее руководитель (председатель). После проведения изучения и анализа материалов, подготовленных для открытого опубликования, экспертная комиссия осуществляет подготовку заключения, в котором формируется мнение экспертной комиссии о возможности (невозможности) открытого опубликования материалов. Экспертное заключение подписывается всеми членами экспертной комиссии, ее руководителем (председателем) и утверждается руководителем предприятия-организатора экспертизы. Форма заключения представлена в приложении 5.

При отсутствии единого мнения экспертов и невозможности вынесения (формулирования) вывода по результатам изучения материалов вопрос о возможности опубликования решается руководителем вышестоящего предприятия (органа государственной власти). В исключительных случаях, при отсутствии вышестоящей организации (органа государственной власти) решение о возможности открытого опубликования материалов выносится руководителем предприятия совместно с руководителем предприятия - заказчиком проводимых совместных работ.

После оформления заключения экспертной комиссии при условии принятия положительного решения о возможности открытого опубликования материалов, оно в установленном порядке вместе с рассмотренными материалами передается в службу безопасности (подразделение по защите государственной тайны) предприятия или уполномоченному должностному лицу для принятия окончательного решения.

После получения разрешения данных подразделений (должностного лица) подготовленные материалы в установленном порядке передаются в издательство (редакцию, представителям средств массовой информации) для опубликования (открытого распространения).

9.6. Основы организации защиты информации в ходе взаимодействия со средствами массовой информации

Правовое закрепление общих принципов свободы массовой информации, механизм организации и деятельности средств массовой информации (СМИ) закреплено в Законах РФ "О средствах массовой информации"[48], "Об авторском праве и смежных правах"[49], Федеральном законе РФ "О порядке освещения деятельности органов государственной власти в государственных средствах массовой информации"[50] и другие законодательные и подзаконные акты.

В статье 1 Закона РФ "О средствах массовой информации" под свободой массовой информации законом понимается не подлежащая ограничениям деятельность по поиску, получению, производству и распространению массовой информации, учреждению средств массовой информации, владению, пользованию и распространению или изготовлению, приобретению, хранению и эксплуатации технических средств и оборудования, сырья и материалов, предназначенных для производства и распространения продукции средств массовой информации. Поэтому недопустимо использовать свободу массовой информации для

[48] Закон РФ от 27.12.1991 г. № 2124-I "О средствах массовой информации".
[49] Закон РФ от 9.07.1993 г. № 5351-I "Об авторском праве и смежных правах".
[50] Федеральный закон РФ от 13.01.1995 г. № 7-ФЗ "О порядке освещения деятельности органов государственной власти в государственных средствах массовой информации".

разглашения сведений, составляющих государственную или иную специально охраняемую законом тайну.

В соответствии со статьей 48 Закона РФ "О средствах массовой информации" редакция имеет право подать заявку в государственный орган, организацию, учреждение, орган общественного объединения на аккредитацию при них своих журналистов, с целью осуществления корреспондентами своей профессиональной деятельности и доступа к источникам информации.

Аккредитацию можно разделить на:

постоянную (на весь срок объявленной аккредитации для журналистов, постоянно освещающих деятельность аккредитующего органа);

временную (ограниченную меньшим сроком для журналистов, выполняющих конкретное задание своих редакций по освещению работы аккредитующего органа);

специальную (при особом режиме мероприятия);

разовую (на одно мероприятие).

Аккредитация представляет реальные выгоды, как для средств массовой информации, так и для предприятий. Первым она помогает в выполнении своей ключевой функции - искать и представлять обществу информацию, вторым - упорядочить работу с журналистами, выработать наиболее приемлемые для каждой организации правила взаимодействия со средствами массовой информации.

Журналист может быть лишен аккредитации только в двух случаях: если им или редакцией нарушены правила аккредитации; если журналистом распространены не соответствующие действительности, порочащие честь и достоинство аккредитовавшей организации сведения, что должно быть подтверждено вступившим в законную силу решением суда.

Никакие иные случаи, в том числе связанные с "необъективностью", "тенденциозностью" освещения, не могут служить основанием для лишения аккредитации.

Конкуренция средств массовой информации на информационном рынке, эйфория некоторых журналистов от сознания своей реальной силы как "четвертой власти" (после законодательной, исполнительной и судебной), наконец, порой их недостаточная компетентность, а также ощущение безнаказанности за ошибки могут привести к многочисленным нарушениям правовых и этических норм.

Если представителем средств массовой информации проведено искажение информации, попраны честь и достоинство гражданина, то свою защиту можно реализовать следующими путями:

- потребовать от редакции опровержения в средствах массовой информации без обращения в суд или в порядке гражданского судопроизводства (статья 152 Гражданского кодекса РФ, статьи 43 и 44 Закона РФ "О средствах массовой информации");

- воспользоваться правом на ответ (реплику, комментарий) согласно статье 46 Закона РФ "О средствах массовой информации";

- привлечь журналиста к уголовной ответственности по статье 129 (клевета) и (или) статье 130 (оскорбление) Уголовного кодекса РФ.

Статья 47 Закона РФ "О средствах массовой информации" четко определяет сферу деятельности журналистов: собирать, обрабатывать и распространять

социально значимую информацию. Для этого они наделены правом посещать государственные органы и организации, предприятия и учреждения, органы общественных объединений либо их пресс-службы; быть принятым должностными лицами в связи с запросом информации; получать доступ к документам и материалам, за исключением их фрагментов, содержащих сведения, составляющие государственную, коммерческую или иную специально охраняемую законом тайну; посещать специально охраняемые места стихийных бедствий, аварий и катастроф, массовых беспорядков и массовых скоплений граждан, а также местности, в которых объявлено чрезвычайное положение; присутствовать на митингах и демонстрациях.

Вместе с тем статья 49 Закона РФ "О средствах массовой информации" предусматривает и обязанности журналистов: проверять достоверность сообщаемой информации; сохранять конфиденциальность информации и (или) ее источника; при получении информации от граждан и должностных лиц ставить их в известность о проведении аудио- и видеозаписи, кино- и фотосъемки; ставить в известность главного редактора о возможных исках и предъявлении иных предусмотренных законом требований в связи с распространением подготовленного сообщения или материала; предъявлять при осуществлении профессиональной деятельности по первому требованию редакционное удостоверение или иной документ, удостоверяющий личность и правомочия журналиста. Кроме того, статья 51 закона запрещает журналисту использовать свои права в целях сокрытия или фальсификации общественно значимых сведений, распространения слухов под видом достоверных сообщений, а также распространения информации с целью опорочить гражданина или отдельные категории граждан исключительно по признакам пола, возраста, расовой или национальной принадлежности, языка, отношения к религии, профессии, места жительства, работы или в связи с политическими убеждениями.

Наряду с правовыми нормами деятельность журналистов регламентируется также нормами и правилами профессиональной этики[51], которые регулируют отношения между журналистом и аудиторией, журналистом и источником информации, журналистом и автором, журналистом и коллегами по работе и т.д.

Для информирования средств массовой информации и общественности руководителями предприятия целесообразно использовать следующие основные формы работы: подготовка сообщений и пресс-релизов; проведение пресс-конференций и брифингов; посещение объектов журналистами; присутствие журналистов на мероприятиях; официальные комментарии; организация встреч с представителями средств массовой информации.

Подготовка сообщений для средств массовой информации является эффективным способом привлечения внимания широких слоев общественности к проблеме, имеющей важное значение. По жанру и тематике сообщения могут быть самыми разными: интервью с руководителем предприятия, статья эксперта, комментарий ученого, особое мнение предприятия по значимому вопросу.

Пресс-релиз относится к числу самых распространенных способов передачи актуальной информации прессе. После написания его отправляют обычной почтой или по каналам электронной связи в различные периодические издания, на радио и телевидение. Текст также может передаваться информационным

[51] Нормы и правила профессиональной этики сведены в "Кодекс профессиональной этики российского журналиста", который был одобрен Конгрессом журналистов России 23.06.1994 г.

агентствам. Редакции зачастую редактируют пресс-релизы, поэтому всегда следует распространять его полный текст с расчетом на сокращение.

Пресс-конференции или брифинги как наиболее привычные и привлекательные формы информирования журналистов.

Посещение объектов, присутствие журналистов на мероприятиях весьма интересная и эффективная форма работы с журналистами. Посещение может быть инициировано как руководителями предприятия, так и средствами массовой информации. При этом представители средств массовой информации должны увидеть что-нибудь действительно новое и ценное, ради чего стоило совершать поездку.

Официальные комментарии в наши дни стали обычной практикой в государственных органах власти.

Основные правила общения со средствами массовой информации представлены в приложении 6.

10. ОСНОВЫ ЗАЩИТЫ ИНФОРМАЦИИ ПРИ ОСУЩЕСТВЛЕНИИ МЕЖДУНАРОДНОГО СОТРУДНИЧЕСТВА И ВЫЕЗДЕ ПЕРСОНАЛА ПРЕДПРИЯТИЯ ЗА ГРАНИЦУ

10.1. Порядок передачи различных видов конфиденциальной информации иностранным государствам

Изменения последних лет в области внешней политики России проявляются, прежде всего, как рост числа международных контактов, их глубины и многогранности. Информационное обеспечение международных договоренностей, в том числе с использованием сведений, составляющих государственную тайну, и конфиденциальной информации осуществлялось и ранее. Тем не менее, в нынешних условиях развития нашего государства проблема обеспечения должного уровня национальной безопасности для своего решения требует создания стройной организации процесса защиты информации во всех сферах деятельности государства.

Таким образом, вопросы правового регулирования защиты информации в ходе международных отношений, в том числе и сохранности государственной тайны, сейчас приобретают особую актуальность.

Наиболее полно данные вопросы определены в отношении информации, содержащей сведения, составляющие государственную тайну, так как данные сведения в соответствии с Законом РФ "О государственной тайне" защищаются государством, а защита государственной тайны в интересах безопасности государства в соответствии с Конституцией РФ находится в компетенции государства.

В отношении иных видов охраняемой информации, действующие нормативные правовые акты в основном определяют следующие права обладателя информации, относящиеся, в том числе, и к сфере международных отношений:

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

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

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

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

- осуществлять иные действия с информацией или разрешать осуществление таких действий.

В случае если информация не является общедоступной и открытой, ее обладатель при принятии решения о передаче информации иностранному государству (организации) должен руководствоваться законодательными и иными нормативными актами России в области международных отношений, а также положениями заключенного международного договора (соглашения), предусматривающего передачу этой информации.

Непосредственную ответственность за обеспечение защиты информации в ходе международного сотрудничества несут руководители органов государственной власти и предприятий, осуществляющих такое сотрудничество. Практическое выполнение задач по защите информации возлагается на соответствующие структурные подразделения (службы безопасности).

Вместе с тем, защита конфиденциальной информации со стороны государства в лице уполномоченных государственных органов (должностных лиц), распространяется только на ту деятельность по международному информационному обмену, которую осуществляют физические и юридические лица, обладающие лицензией на работу с конфиденциальной информацией и использующие сертифицированные средства международного информационного обмена.

Организация и порядок передачи за границу информации, содержащей сведения, составляющие государственную тайну, определяются Законом РФ "О государственной тайне" и "Положением о подготовке к передаче сведений, составляющих государственную тайну, другим государствам"[52].

10.2. Организация подготовки к передаче сведений, составляющих государственную тайну, другим государствам

При необходимости передачи сведений, составляющих государственную тайну, в рамках международной деятельности другим государствам, решение о передаче сведений в соответствии с Законом РФ "О государственной тайне" принимается Правительством Российской Федерации при наличии экспертного заключения Межведомственной комиссии по защите государственной тайны о возможности передачи этих сведений.

Обязательства принимающей стороны по защите передаваемых ей сведений предусматриваются заключаемым с ней договором[53].

В целях реализации положений законодательства Российской Федерации о государственной тайне и обеспечении при этом ее защиты:

---

[52] Утверждено постановлением Правительства РФ от 2.08.1997 г. № 973.

[53] Под международным договором понимаются международные соглашения независимо от их конкретного наименования, заключаемые Российской Федерацией в соответствии с Федеральным законом РФ от 15.05.1995 г. № 101-ФЗ "О международных договорах Российской Федерации".

Президент Российской Федерации заключает международные договоры Российской Федерации о совместном использовании и защите сведений, составляющих государственную тайну;

Правительство Российской Федерации заключает межправительственные соглашения, принимает меры по выполнению международных договоров Российской Федерации о совместном использовании и защите сведений, составляющих государственную тайну, принимает решения о возможности передачи их носителей другим государствам.

Межведомственная комиссия по защите государственной тайны в соответствии с "Положением о Межведомственной комиссии по защите государственной тайны"[54] выполняет следующие функции:

- рассматривает вопросы о возможности передачи сведений, составляющих государственную тайну, другим государствам и международным организациям и представляет в установленном порядке в Правительство Российской Федерации соответствующие экспертные заключения;

- рассматривает по поручениям Президента Российской Федерации и Правительства Российской Федерации проекты международных договоров Российской Федерации о совместном использовании и защите сведений, составляющих государственную тайну, организует разработку соответствующих предложений и экспертных заключений, участвует в международном сотрудничестве по этим вопросам.

В рамках международной деятельности под передачей сведений, составляющих государственную тайну, другим государствам понимается доведение до иностранного государства (уполномоченного государством представителя) каким-либо способом (передача, пересылка, ознакомление, осуществление доступа) указанных сведений.

При возникновении необходимости передачи сведений, составляющих государственную тайну, другим государствам, заинтересованные в передаче сведений федеральные органы исполнительной власти, органы исполнительной власти субъектов Российской Федерации и предприятия направляют руководителям органов государственной власти, наделенным полномочиями по распоряжению сведениями, мотивированное ходатайство.

В мотивированном ходатайстве 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.

[54] Утверждено Указом Президента РФ от 6.10.2004 г. № 1286.

Мотивированное ходатайство, решение органа государственной власти, руководитель которого наделен полномочиями по распоряжению сведениями, а также действующие (ранее заключенные) международные договоры и другие документы, имеющие непосредственное отношение к защите рассматриваемых к передаче сведений, заявитель представляет в Межведомственную комиссию по защите государственной тайны для подготовки экспертного заключения.

При положительном экспертном заключении Межведомственной комиссии по защите государственной тайны и наличии вывода о возможности передачи сведений иностранному государству, оно в установленный срок направляется органу государственной власти (организации), заинтересованному в передаче сведений, составляющих государственную тайну.

По ходатайству органа государственной власти (организации), заинтересованного в передаче сведений, составляющих государственную тайну, орган государственной власти, руководитель которого наделен полномочиями по распоряжению сведениями, проект соответствующего решения Правительства Российской Федерации с экспертным заключением Межведомственной комиссии по защите государственной тайны вносится в установленном порядке в Правительство Российской Федерации.

После принятия Правительством Российской Федерации этого решения заинтересованный орган государственной власти совместно с Министерством иностранных дел Российской Федерации, Федеральной службой безопасности Российской Федерации и органом государственной власти, в чьем распоряжении находятся данные сведения, в порядке, установленном законодательством России, осуществляют подготовку проекта межправительственного договора (соглашения) о взаимной защите передаваемых сведений.

Данный проект в установленном порядке передается на рассмотрение иностранному государству, с которым осуществляется международное сотрудничество в данной области и которому предполагается передача сведений, составляющих государственную тайну.

Проект договора (соглашения) должен содержать:

- обязательства принимающей стороны по защите передаваемых ей сведений;

- 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 об их защите в соответствии с внутренним законодательством принимающей стороны;

- порядок разрешения конфликтных ситуаций и возмещения возможного ущерба.

В случае отказа государства-получателя сведений от заключения международного договора о взаимном обеспечении их защиты в Правительство Российской Федерации представляется информация о ранее принятых на себя обязательствах и гарантиях принимающей стороны по обеспечению защиты переда-

ваемых ей в рамках данного международного сотрудничества сведений, а также их нераспространению третьим странам.

На основании решения Правительства Российской Федерации в соответствии с процедурами, предусмотренными международным договором и действующими нормативными правовыми актами, осуществляется фактическая передача сведений, составляющих государственную тайну, и (или) их носителей.

Фактическую передачу сведений, составляющих государственную тайну, иностранному государству осуществляет уполномоченный орган государственной власти или организация, которым это поручено в соответствии с заключенным международным договором или Правительством Российской Федерации в рамках его реализации.

Передача носителей сведений, составляющих государственную тайну, осуществляется на основании заключенного контракта на их поставку (передачу) или на поставку продукции, товаров или услуг, в которых они содержатся.

В этих контрактах могут предусматриваться дополнительные меры защиты передаваемых сведений.

Руководители органов государственной власти и организаций, уполномоченных Правительством Российской Федерации осуществлять передачу сведений (их носителей) другим государствам, несут ответственность за нарушение или ненадлежащее исполнение законодательства Российской Федерации о государственной тайне.

Контроль порядка реализации положений международного договора о взаимной защите сведений, составляющих государственную тайну, заключенного Российской Федерацией с иностранным государством, которому они передаются (переданы) осуществляется органом государственной власти, определенным в этом договоре (компетентным органом).

10.3. Ограничения прав гражданина, осведомленного в сведениях, составляющих государственную тайну, на выезд за границу

В соответствии с Законом РФ "О государственной тайне" допуск должностных лиц и граждан к государственной тайне предусматривает письменное согласие на частичные, временные ограничения их прав, в том числе ограничение права выезда за границу на срок, оговоренный в трудовом договоре (контракте), заключенном при оформлении допуска к государственной тайне.

Право гражданина на выезд из Российской Федерации может быть временно ограничено в случае, если он при допуске к сведениям особой важности или совершенно секретным сведениям, в установленном порядке отнесенным к государственной тайне, заключил трудовой договор (контракт), предполагающий временное ограничение права на выезд из Российской Федерации[55].

Срок ограничения устанавливается Федеральным законом РФ "О порядке выезда из Российской Федерации и въезда в Российскую Федерацию"[56] и не может превышать пяти лет со дня последнего ознакомления лица со сведениями особой важности или совершенно секретными сведениями. Ограничение граж-

[55] Для граждан, допущенных к секретным сведениям, право на выезд из Российской Федерации не ограничено.

[56] Федеральный закон РФ от 15.08.1996 г. № 114-ФЗ "О порядке выезда из Российской Федерации и въезда в Российскую Федерацию".

данина в праве на выезд из Российской Федерации по данному основанию действует до истечения срока действия ограничения, установленного трудовым договором (контрактом).

Срок ограничения права на выезд из Российской Федерации может быть продлен Межведомственной комиссией, образуемой Правительством Российской Федерации[57], на основании заключения Межведомственной комиссии по защите государственной тайны. Данное заключение формируется на основе мотивированного ходатайства органа государственной власти, наделенного полномочиями по распоряжению сведениями, составляющими государственную тайну, о том, что сведения, в которых гражданин был осведомлен на день подачи заявления о выезде из Российской Федерации, сохраняют соответствующую степень секретности.

Установленный этой Межведомственной комиссией срок ограничения права на выезд гражданина из Российской Федерации не может превышать в общей сложности десяти лет, включая срок ограничения, установленный трудовым договором (контрактом), со дня последнего ознакомления лица со сведениями особой важности или совершенно секретными сведениями.

В случае если гражданин сообщил о себе заведомо ложную информацию, включая информацию о допуске его к сведениям, составляющим государственную тайну, имеющим степень секретности "особой важности" или "совершенно секретно", его право на выезд за границу до решения данного вопроса может быть временно ограничено органом, оформляющим документы на выдачу заграничного паспорта (но на срок не более одного месяца).

Основанием для временного ограничения права на выезд из Российской Федерации работников, допущенных (ранее допускавшихся) к сведениям особой важности или совершенно секретным сведениям, является принимаемое уполномоченными должностными лицами решение о временном ограничении их права на выезд из Российской Федерации.

Такое решение принимается:

- в отношении работников предприятий, подведомственных федеральным органам исполнительной власти, - руководителями этих федеральных органов;

- в отношении работников предприятий, не входящих в структуру федерального органа исполнительной власти, находящихся на территории субъекта Российской Федерации, - руководителями органов исполнительной власти субъектов Российской Федерации.

Решения об ограничении права на выезд из Российской Федерации граждан, осведомленных о сведениях особой важности или совершенно секретных сведениях, отнесенных к государственной тайне, могут быть ими обжалованы в Межведомственную комиссию, образуемую Правительством Российской Федерации, которая обязана рассмотреть жалобу и дать ответ не позднее чем в трехмесячный срок. Отказ гражданину Российской Федерации в праве на выезд из Российской Федерации может быть обжалован в суд.

В случае если выезд из Российской Федерации гражданина Российской Федерации ограничен по основанию, связанному с допуском и фактической работой со сведениями, имеющими степень секретности "особой важности" или "совершенно секретно", его паспорт подлежит передаче на хранение до истече-

[57] Постановление Правительства РФ от 1.06.2004 г. № 260 "О Регламенте Правительства Российской Федерации и Положении об Аппарате Правительства Российской Федерации".

ния срока временного ограничения в государственный орган, осуществивший выдачу паспорта.

10.4. Работа должностных лиц предприятия по оформлению документов на выезд сотрудников в служебные командировки и по частным делам

В целях выявления законных оснований для возможного временного ограничения права гражданина на выезд за границу, государственный орган, осуществляющий оформление документа, удостоверяющего личность гражданина, по которому он осуществляет выезд из Российской Федерации, осуществляет согласование вопроса выезда этого гражданина за границу с соответствующим органом Федеральной службы безопасности Российской Федерации (далее - орган безопасности).

Данный орган безопасности проработку вопроса о возможности выезда за границу гражданина осуществляет совместно с предприятиями, в которых этот гражданин работал в течение последних десяти лет (или работает на момент оформления заграничного паспорта).

При получении запроса органа безопасности руководитель предприятия обязан в установленный срок организовать рассмотрение вопроса о возможности выезда его сотрудника за границу.

При этом изучается наличие допуска у данного сотрудника к государственной тайне, заключенного договора (контракта) об оформлении такого допуска, а также реальное ознакомление его со сведениями особой важности или совершенно секретными сведениями.

В случае если работник предприятия осведомлен в "особой важности" или "совершенно секретных" сведениях, он на основании письменного вывода (заключения) о его фактической осведомленности в этих сведениях, может быть ограничен в праве на выезд за границу. Это заключение оформляется подразделением, в котором работает гражданин совместно с подразделением по защите государственной тайны и утверждается руководителем предприятия.

Однако решение об ограничении права на выезд работника за границу с учетом подготовленного вывода (заключения) может быть принято только в случае, если он при допуске к сведениям "особой важности" или "совершенно секретным" сведениям заключил договор (контракт), предполагающий временное ограничение гражданина в этом праве.

Срок ограничения права на выезд, подтверждаемый соответствующим решением уполномоченного должностного лица, исчисляется с момента его последнего письменного ознакомления с соответствующими сведениями.

Вместе с тем, работник предприятия в силу своих должностных (функциональных) обязанностей и возложенных на него задач, может быть направлен для решения служебных вопросов в служебную командировку за границу в составе делегации своего предприятия или в составе делегации органа государственной власти (органа местного самоуправления).

В этом случае данному работнику уполномоченными органами государственной власти, в составе делегаций которых предполагается командирование работника предприятия, оформляется служебный паспорт. Вопрос выезда за границу этого работника также в установленном порядке согласовывается с органом безопасности.

Выезд за границу в служебную командировку работников, фактически осведомленных в особой важности или совершенно секретных сведениях, возможен только в случае крайней необходимости, когда направить в эту служебную командировку лиц, менее осведомленных в сведениях, составляющих государственную тайну, не представляется возможным.

Руководители предприятий, работники которых выезжают за границу в служебные командировки и по частным делам, обязаны проинструктировать их по правилам поведения в стране пребывания. Эти руководители предупреждают работников о недопущении распространения (разглашения) ими сведений, составляющих государственную тайну, за исключением случаев, когда это предусмотрено программой пребывания (служебной командировки) на предприятии, осуществляющем (планирующем) совместные работы с предприятием, командировавшим работника.

11. ДОПУСК ПРЕДПРИЯТИЙ К ПРОВЕДЕНИЮ РАБОТ С КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИЕЙ

11.1. Основные положения лицензирования деятельности предприятий, связанной с использованием сведений, составляющих государственную тайну

В соответствии с Законом РФ "О государственной тайне" допуск к государственной тайне предприятий, учреждений и организаций - это оформление их права на проведение работ с использованием сведений, составляющих государственную тайну.

При осуществлении предприятием работ с использованием сведений, составляющих государственную тайну, необходимо данному предприятию в порядке, установленном нормативными правовыми актами и методическими документами, получить лицензию на осуществление этого вида деятельности.

В сфере защиты государственной тайны установлены следующие виды деятельности, подлежащие лицензированию:

- проведение работ, связанных с использованием сведений, составляющих государственную тайну (см. рисунок 11.1);
- проведение работ, связанных с созданием средств защиты информации (см. рисунок 11.2);
- проведение работ, связанных с осуществлением мероприятий и (или) оказанием услуг в области защиты государственной тайны (в части технической защиты информации) (см. рисунок 11.3).

Необходимо обратить внимание, что незаконная деятельность в области защиты информации без наличия соответствующих лицензий, а, равно как и нарушение условий работы, предусмотренных лицензией, является наказуемым деянием, и руководители предприятий и должностные лица службы безопасности несут административную ответственность по статьям 13.13 и 13.12 (соответственно) Кодекса РФ об административных правонарушениях (см. приложение 10).

ЛИЦЕНЗИЯ

Б 319286

Регистрационный номер 1114 от «30» августа 2000г.

Центр ФСБ России по лицензированию, сертификации и защите государственной тайны

разрешает осуществление работ с использованием сведений, составляющих государственную тайну, при условии обслуживания РСО АООТ "Телеком"

Лицензия выдана Обществу с ограниченной ответственностью "Стил - Компьютерные системы" (113095, г. Москва, ул. Пятницкая, д. 34, стр. 2)

Условия осуществления данного вида деятельности соблюдение требований законодательных и иных нормативных актов Российской Федерации по обеспечению защиты сведений, составляющих государственную тайну.

Срок действия лицензии до 03 февраля 2004 года

М. П. Подпись В.М. Гладышев

Лицензия продлена до «__» _____ 199__ г.

М. П. Подпись

Сведения о регистрации лицензии на территориях субъектов Российской Федерации

М. П. Подпись

Выдается предприятиям и организациям осуществляющих работы с использованием сведений, составляющих государственную тайну (имеющих режимно-секретные органы).

Описание: бланк салатного цвета из плотной специальной бумаги; герб: орел черный, фон желтый; водяные знаки темно-зеленого цвета; гербовая печать синего цвета; серия и номер красного цвета.

Рис. 11.1. Образец лицензии ФСБ РФ на осуществление работ с использованием сведений, составляющих государственную тайну

СЕРИЯ ГТ 0030 НОМЕР 001453

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ

ЛИЦЕНЗИЯ

НА ПРОВЕДЕНИЕ РАБОТ, СВЯЗАННЫХ С СОЗДАНИЕМ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

Регистрационный номер 1765 от 13 сентября 2005 г.

Лицензия выдана Обществу с ограниченной ответственностью «Лаборатория испытаний средств и систем информатизации»

117418, г. Москва, ул. Гарибальди, дом 36, секция 9
код ОКПО - 58169198

Перечень работ, связанных с созданием средств защиты информации, на которые распространяется настоящая лицензия:

разработка, производство, реализация, установка, монтаж, наладка, испытания, ремонт, сервисное обслуживание:

технических средств защиты информации;
защищенных технических средств обработки информации;
технических средств контроля эффективности мер защиты информации;
программных (программно-технических) средств защиты информации;
защищенных программных (программно-технических) средств обработки информации;
программных (программно-технических) средств контроля защищенности информации.

Лицензия действительна до 13 сентября 2008 г.

Начальник управления

М.П. В. Селин

Выдается предприятиям и организациям на проведение работ, связанных с созданием средств защиты информации.

Описание: бланк светло-серого цвета из плотной специальной бумаги; герб: орел черный, щит триколор; водяные знаки голубоватого цвета; гербовая печать синего цвета; серия: буквы красного цвета, цифры черного цвета, номер черного цвета; на обороте расшифровка перечня разрешенных работ.

Рис. 11.2. Образец лицензии ФСТЭК РФ на проведение работ, связанных с созданием средств защиты информации

СЕРИЯ ГТ 0030 НОМЕР 001452

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ

ЛИЦЕНЗИЯ

НА ОСУЩЕСТВЛЕНИЕ МЕРОПРИЯТИЙ И (ИЛИ) ОКАЗАНИЕ УСЛУГ В ОБЛАСТИ ЗАЩИТЫ ГОСУДАРСТВЕННОЙ ТАЙНЫ
(в части технической защиты информации)

Регистрационный номер *1016* *от* *13* *сентября* *2005 г.*

Лицензия выдана Обществу с ограниченной ответственностью
«Лаборатория испытаний средств и систем информатизации»

117418, г. Москва, ул. Гарибальди, дом 36, секция 9
код ОКПО - 58169198

Перечень мероприятий и услуг в области защиты государственной тайны, на которые распространяется настоящая лицензия:

сертификационные испытания (программных (программно-технических) средств защиты информации; защищенных программных (программно-технических) средств обработки информации; программных (программно-технических) средств контроля защищенности информации);

проектирование объектов в защищенном исполнении (автоматизированных систем различного уровня и назначения; систем связи, приема, обработки и передачи данных; систем отображения и размножения).

Лицензия действительна до *13* *сентября* *2008 г.*

Начальник управления

В. Селин

Выдается предприятиям и организациям, на осуществление мероприятий и (или) оказание услуг в области защиты государственной тайны (в части технической защиты информации).

Описание: бланк светло-серого цвета из плотной специальной бумаги; герб: орел черный, щит триколор; водяные знаки голубоватого цвета; гербовая печать синего цвета; серия: буквы красного цвета, цифры черного цвета, номер черного цвета; на обороте расшифровка перечня разрешенных работ.

Рис. 11.3. Образец лицензии ФСТЭК РФ на осуществление мероприятий и (или), оказание услуг в области защиты государственной тайны

Порядок организации и проведения работ по лицензированию деятельности предприятий в сфере защиты государственной тайны определены "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"[58].

Основы понятия лицензирования и общие требования к алгоритму лицензирования, функции и задачи, решаемые лицензирующими органами, права и обязанности соискателей лицензий и лицензиатов, определены Федеральным законом РФ "О лицензировании отдельных видов деятельности"[59] и постановлением Правительства РФ "Об организации лицензирования отдельных видов деятельности"[60].

Однако, в соответствии с пунктом 2 данного федерального закона, его действие не распространяется на деятельность, связанную с защитой государственной тайны.

Органами, уполномоченными на ведение лицензионной деятельности в сфере защиты государственной тайны, 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).

Вместе с тем, лицензирование деятельности предприятий Федеральной службы безопасности Российской Федерации, Министерства обороны 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, осуществляется руководителями министерств и ведомств Российской Федерации, которым подчинены указанные предприятия.

В настоящем учебном пособии будет рассмотрен лишь один из вышеперечисленных видов лицензирования - лицензирование на допуск предприятий к проведению работ, связанных с использованием сведений, составляющих государственную тайну. Это объясняется тем, что этот вид деятельности является

[58] Утверждено постановлением Правительства РФ от 15.03.1995 г. № 333.

[59] Федеральный закон РФ от 8.08.2001 г. № 128-ФЗ "О лицензировании отдельных видов деятельности".

[60] Утверждено постановлением Правительства РФ от 26.01.2006 г. № 45.

основным и охватывает все без исключения предприятия, выполняющие такие работы. Тогда как два остальных вида деятельности могут осуществляться предприятием только при наличии у него лицензии на проведение работ со сведениями, составляющими государственную тайну. Кроме того, работы по этим двум видам, в силу специфики их выполнения, проводят лишь некоторые предприятия, отвечающие соответствующим требованиям. Особенности лицензирования этих видов деятельности в большей степени определены ведомственными нормативными актами федеральных органов исполнительной власти, которым Правительством Российской Федерации предоставлено право оформления и выдачи соответствующих лицензий.

11.2. Алгоритм работы лицензирующего органа по лицензированию деятельности предприятий

Лицензии на проведение работ, связанных с использованием сведений, составляющих государственную тайну, выдаются предприятиям 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.

Лицензии оформляются на бланках, имеющих степень защиты, соответствующую степени защиты ценной бумаги на предъявителя. Лицензия подписывается руководителем (заместителем руководителя) органа, уполномоченного на ведение лицензионной деятельности, и заверяется печатью этого органа. Копия лицензии хранится в органе, уполномоченном на ведение лицензионной деятельности.

Срок действия лицензии не может быть менее трех и более пяти лет, однако по просьбе заявителя лицензии могут выдаваться на срок менее трех лет.

Для получения лицензии соискатель лицензии представляет в соответствующий орган, уполномоченный на ведение лицензионной деятельности заявление о выдаче лицензии с приложением копий уставных и учредительных документов, а также при необходимости и других материалов, характеризующих деятельность предприятия.

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.

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.

Для проведения специальных экспертиз органы, уполномоченные на ведение лицензионной деятельности, создают аттестационные центры, которые получают соответствующие лицензии на право их проведения. Для проведения специальных экспертиз могут создаваться аттестационные центры в органах власти, руководители которых наделены полномочиями по отнесению сведений к государственной тайне, а также в субъектах Российской Федерации.

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

Перечни вопросов, подлежащих проверке в ходе специальной экспертизы предприятия, определяются нормативно-методическими документами, утверждаемыми органами, уполномоченными на ведение лицензионной деятельности, а также программами специальных экспертиз предприятий, разрабатываемыми уполномоченными лицензирующими органами и утверждаемыми их руководителями.

В ходе специальной экспертизы проводится оценка готовности выполнения предприятием требований законодательных и иных нормативных актов Российской Федерации по обеспечению защиты сведений, составляющих государственную тайну, в процессе выполнения работ, связанных с использованием этих сведений.

Оценка готовности предусматривает проверку:

- наличия нормативных актов и нормативно-методических документов по направлениям защиты государственной тайны: режим секретности; противодействие иностранным техническим разведкам; защита информации от утечки по техническим каналам;

- наличия и качества разработки предприятием документов, регламентирующих организацию и порядок проведения на предприятии работ по защите сведений, составляющих государственную тайну;

- наличия в структуре предприятия подразделения по защите государственной тайны;

- наличия аттестованных объектов информатики (кроме органов шифровальной службы).

Одним из важных вопросов, подлежащих проверке при проведении специальной экспертизы, является проверка наличия в структуре необходимого числа специально подготовленных сотрудников для работы по защите государственной тайны и уровня их квалификации. В ходе проверки этих вопросов оценивается готовность сотрудников предприятия выполнять следующие виды работ:

- определение охраняемых сведений, демаскирующих признаков предприятия и его производственной деятельности;
- проведение анализа возможностей технической разведки в отношении предприятия по добыванию сведений, составляющих государственную тайну;
- выявление каналов утечки сведений, составляющих государственную тайну;
- разработка мероприятий по защите сведений, составляющих государственную тайну, и оценка их достаточности;
- аттестование рабочих мест по всему производственному циклу разработки и испытания продукции, товаров и предоставления услуг, связанных с использованием сведений, составляющих государственную тайну;
- контроль эффективности выполнения мероприятий по защите государственной тайны.

Результаты специальной экспертизы оформляются актом, который докладывается руководителю уполномоченного лицензирующего органа и учитывается при принятии решения о выдаче лицензии.

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.

Сроки рассмотрения заявлений, проведения специальной экспертизы, порядок и сроки принятия решения о выдаче, аннулировании, приостановлении и возобновлении действия лицензии определяются "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".

Контроль за соблюдением лицензионных требований и условий лицензиатами, выполняющими работы, связанные с использованием сведений, составляющих государственную тайну, осуществляют органы, уполномоченные на ведение лицензионной деятельности.

Руководители и должностные лица органов, уполномоченных на ведение лицензионной деятельности, несут ответственность за нарушение или ненадлежащее исполнение положений нормативных актов в области лицензирования деятельности предприятий, связанных с использованием сведений, составляющих

государственную тайну, в соответствии с законодательством Российской Федерации.

Предприятия и их должностные лица в соответствии с Кодексом РФ об административных правонарушениях несут ответственность за осуществление деятельности, связанной с использованием сведений, составляющих государственную тайну, без лицензии, а также за нарушение условий, предусмотренных лицензией на осуществление этого вида деятельности (см. приложение 10).

11.3. Организация проведения государственной аттестации руководителей предприятий

Государственная аттестация руководителей предприятий организуется органами, уполномоченными на ведение лицензионной деятельности, а также министерствами и ведомствами Российской Федерации, 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"[61] разрабатываются и утверждаются Межведомственной комиссией по защите государственной тайны.

Государственная аттестация руководителей предприятий организуется Федеральной службой безопасности Российской Федерации и ее территориальными органами (на территории Российской Федерации), Службой внешней разведки Российской Федерации (за рубежом), Федеральной службой по техническому и экспортному контролю, а также органами государственной власти, руководители которых наделены полномочиями по отнесению сведений к государственной тайне (в пределах компетенции).

Вышеперечисленными государственными органами могут разрабатываться положения о государственной аттестации руководителей предприятий, ответственных за защиту сведений, составляющих государственную тайну, учитывающие специфику их деятельности.

Государственная аттестация руководителей предприятий проводится с целью оценки знаний аттестуемого лица, необходимых для организации на предприятии защиты сведений, составляющих государственную тайну.

Государственная аттестация проводится методом собеседования. Она, как правило, осуществляется аттестационной комиссией, создаваемой для проведения специальной экспертизы предприятия.

Аттестуемое лицо обязано знать:

- 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 организации защиты государственной тайны на предприятии.

Расходы по государственной аттестации руководителей предприятий относятся на счет предприятий.

От государственной аттестации освобождаются руководители предприятий, имеющие свидетельства об окончании учебных заведений, уполномоченных

[61] Утверждены решением Межведомственной комиссии по защите государственной тайны от 13.03.1996 г. № 3.

осуществлять подготовку специалистов по вопросам защиты информации, составляющей государственную тайну. Перечень указанных учебных заведений утверждается Межведомственной комиссией по защите государственной тайны по представлению органов, уполномоченных на ведение лицензионной деятельности[62].

При освобождении от занимаемой должности (увольнения) аттестованного в ходе лицензирования предприятия руководителя, ответственного за защиту сведений, составляющих государственную тайну, вновь назначенный руководитель предприятия должен пройти государственную аттестацию не позднее 3-х месячного срока после его назначения на эту должность.

Результаты государственной аттестации руководителя предприятия включаются в акт проведения специальной экспертизы или оформляются отдельным актом, который представляется экспертной комиссии при проведении экспертизы предприятия. Они учитываются при принятии решения о выдаче предприятию лицензии на проведение работ, связанных с использованием сведений, составляющих государственную тайну.

12. ОРГАНИЗАЦИЯ АНАЛИТИЧЕСКОЙ РАБОТЫ И КОНТРОЛЯ СОСТОЯНИЯ ЗАЩИТЫ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

Анализ состояния защиты информации - это комплексное, органически взаимосвязанное изучение фактов, событий, процессов, явлений, связанных с проблемами защиты охраняемой информации; исследование данных проблем путем обработки информации о состоянии работы по выявлению возможных каналов утечки информации, о причинах и обстоятельствах, способствующих утечке и нарушениям режима секретности (конфиденциальности) в ходе повседневной деятельности предприятия.

Аналитическая работа на предприятии организуется и проводится с целью накопления, обобщения и исследования информации, материалов, фактов и событий, связанных с проблемами защиты конфиденциальной информации.

Основное предназначение аналитической работы - выработка эффективных мер, предложений и рекомендаций руководству предприятия, направленных на недопущение утечки сведений с ограниченным доступом о деятельности предприятия и проводимых работах.

Осуществляемые в ходе этой работы системное получение, анализ и накопление информации должны включать в себя элементы прогнозирования возможных действий противника по получению важной защищаемой информации.

Основными направлениями аналитической работы на предприятии являются:

- анализ объекта защиты;
- анализ внутренних и внешних угроз;
- анализ возможных каналов несанкционированного доступа к информации;

[62] Перечень учебных заведений, осуществляющих подготовку специалистов по защите информации, свидетельство об окончании которых дает руководителям предприятий, учреждений и организаций право на освобождение от государственной аттестации, утвержден решением Межведомственной комиссии по защите государственной тайны от 21.10.1998 г. № 41.

- анализ системы комплексной безопасности объектов;

- анализ имеющих место нарушений режима конфиденциальности информации;

- анализ предпосылок к разглашению информации, а также к утрате носителей конфиденциальной информации[63] и т.д.

Функции аналитического характера на предприятии возлагаются на специально создаваемое в его структуре аналитическое подразделение, укомплектованное квалифицированными специалистами в области защиты информации. Вместе с тем, данные специалисты должны в полной мере владеть информацией по всем направлениям деятельности предприятия: знать виды, характер и последовательность выполнения производственных работ, взаимодействующие организации, специфику деятельности структурных подразделений предприятия и т.д.

Как правило, аналитическое подразделение структурно включается в состав службы безопасности предприятия.

Аналитическое подразделение должно быть единой и взаимосвязанной структурой обеспечения руководства предприятия достоверной и аналитически обработанной информацией, направленной на полноценную информационную поддержку принятия эффективных управленческих решений по всем направлениям информационной безопасности.

Основными функциями такого подразделения являются:

- обеспечение своевременного поступления достоверной и всесторонней информации по проблемным вопросам защиты конфиденциальной информации;

- моделирование реального сценария возможных действий предприятий-конкурентов (противника), которые могут затрагивать интересы предприятия;

- осуществление постоянного мониторинга событий и фактов на рынке продукции, товаров и услуг, а также во внешней среде, которые могут иметь значение для деятельности предприятия;

- обеспечение безопасности собственных информационных ресурсов;

- обеспечение эффективности работы по анализу имеющейся информации, исключение дублирования при ее сборе, обработке и распространении;

- подготовка выводов и предложений на основе проводимой работы в сфере информационной безопасности.

Одним из основных источников поступающей для изучения, обобщения и обработки информации являются материалы контроля состояния защиты конфиденциальной информации на предприятии.

Контроль - целенаправленная деятельность руководства и должностных лиц предприятия по проверке состояния защиты конфиденциальной информации в ходе его повседневной деятельности при выполнении предприятием всех видов работ.

Контроль состояния защиты конфиденциальной информации на предприятии организуется и проводится с целью определения истинного состояния дел по вопросам защиты информации, оценки эффективности принимаемых для исключения утечки информации мер, выявления возможных каналов утечки сведений, выработки предложений и рекомендаций руководству предприятия по совершенствованию комплексной системы защиты информации.

---

[63] Под носителями конфиденциальной информации понимаются документы, материалы, изделия, магнитные носители, содержащие сведения конфиденциального характера.

Указанный контроль осуществляется в порядке и в сроки, определенные нормативными правовыми актами и методическими документами, как вышестоящими органами государственной власти (министерством или ведомством), так и должностными лицами предприятия.

Организация контроля непосредственно на предприятии, в том числе входящих в его структуру подразделениях, возлагается на руководителя предприятия или его заместителя, возглавляющего работу по защите информации на предприятии.

Непосредственная организация и осуществление контроля состояния конфиденциальной информации возлагаются на службу безопасности предприятия или структурное подразделение по защите государственной тайны (режимно-секретное подразделение) предприятия.

Контроль состояния защиты конфиденциальной информации на предприятии осуществляется в форме проверок.

По характеру (способу проведения) проверки подразделяются на плановые и внезапные проверки, а по объему проведения - на комплексные и частные проверки. Плановые проверки организуются заблаговременно, включаются в соответствующие планы мероприятий предприятия на календарный год и месяц. Внезапные проверки организуются и проводятся в необходимых случаях по указанию руководителя предприятия или его заместителя. Они могут проводиться как в масштабах предприятия, так и в его структурных подразделениях, филиалах или представительствах.

Комплексные проверки организуются и проводятся по всем направлениям защиты конфиденциальной информации. К их проведению привлекаются все структурные подразделения, отвечающие за вопросы защиты информации на предприятии. Комплексные проверки охватывают все сферы повседневной деятельности предприятия (его структурного подразделения, филиала или представительства) и имеют своей целью всестороннюю оценку состояния дел с защитой информации.

Основными задачами контроля являются:

- проверка наличия носителей конфиденциальной информации;
- соблюдение всеми сотрудниками предприятия норм и правил, устанавливающих порядок обращения с носителями конфиденциальной информации;
- анализ состояния дел по вопросам защиты информации в структурных подразделениях (в том числе в филиалах и представительствах предприятия);
- выявление угроз защите конфиденциальной информации и выработка мер по их нейтрализации;
- оказание практической помощи должностным лицам в приведении проверяемых вопросов в соответствие требованиям нормативно-методических документов;
- принятие мер административной и дисциплинарной ответственности к лицам, нарушающим требования по порядку обращения с носителями конфиденциальной информации;
- проверка эффективности мер, принимаемых должностными лицами и руководителями структурных подразделений предприятия по защите конфиденциальной информации.

Особое внимание в ходе контроля уделяется вопросам хранения и обращения с носителями конфиденциальной информации на территориально обособленных объектах предприятия, находящихся на удалении.

В ходе проверки наличия носителей конфиденциальной информации проверяются: порядок учета, хранения, размножения (копирования) и уничтожения носителей конфиденциальной информации; оборудование помещений, в которых хранятся указанные носители или осуществляется работа с ними, порядок передачи носителей между исполнителями, в том числе и при убытии лиц в командировку (отпуск, на лечение), и другие вопросы.

Проверке подлежат также вопросы допуска и доступа всех категорий должностных лиц к конфиденциальной информации, в том числе и непосредственно к носителям информации, организации и осуществления пропускного и внутриобъектового режимов на предприятии, организации охраны предприятия и его объектов.

С учетом условий и специфики деятельности предприятия, осуществляемых видов деятельности, повышенное внимание уделяется вопросам защиты информации при планировании и проведении предприятием договорных работ, а также при осуществлении международного сотрудничества.

В повседневной деятельности предприятия и его структурных подразделений особое место занимают периодические проверки должностными лицами (соответствующими структурными подразделениями) наличия носителей конфиденциальной информации, проводимые порядком и в сроки, определенные нормативными правовыми актами и методическими документами, регулирующими порядок обращения с информацией различных видов конфиденциальности.

Результаты контроля доводятся до должностных лиц и сотрудников предприятия, изучаются в ходе проведения соответствующих занятий, недостатки и нарушения оперативно устраняются. Они являются основой для проведения аналитической работы и подготовки предложений руководству предприятия с целью выработки конкретных мероприятий по совершенствованию системы защиты конфиденциальной информации и повышению эффективности работы в вопросах организации и обеспечения режима секретности (конфиденциальности).

Наличие, ведение и результаты постоянной аналитической работы определяют необходимость, основы организации, структуру и содержание системы комплексной защиты информации, степень ее требуемой эффективности и направления развития и совершенствования.

От эффективности и качества ведения на предприятии аналитической работы в полной мере зависит состояние защищенности информационных ресурсов предприятия, отнесенных к категории охраняемых, а также своевременность и обоснованность принятия мер по исключению утечки конфиденциальной информации и утрат носителей конфиденциальной информации.

13. ОРГАНИЗАЦИЯ И ПРОВЕДЕНИЕ СЛУЖЕБНОГО РАССЛЕДОВАНИЯ В СЛУЧАЕ РАЗГЛАШЕНИЯ СВЕДЕНИЙ КОНФИДЕНЦИАЛЬНОГО ХАРАКТЕРА ИЛИ УТРАТЫ НОСИТЕЛЕЙ СВЕДЕНИЙ

Разглашение сведений конфиденциального характера - это предание их огласке работником, который в установленном порядке имел допуск к данным сведениям в силу выполнения служебных (должностных) обязанностей, в результате чего они стали достоянием посторонних лиц.

Под утратой носителей сведений конфиденциального характера (документов, материалов, изделий) понимается выход (в том числе на непродолжительное время) носителей сведений из владения работника, который в установленном порядке имел допуск к данным носителям в силу выполнения служебных (должностных) обязанностей, в результате чего они стали либо могли стать достоянием посторонних лиц.

За разглашение сведений конфиденциального характера, утрату носителей этих сведений виновные лица привлекаются к уголовной и административной ответственности. Такая ответственность предусмотрена статьями 275, 283, 284 Уголовного кодекса РФ (см. приложение 9) и статьей 13.14 Кодекса РФ об административных правонарушениях (см приложение 10).

О факте разглашения сведений конфиденциального характера, или утраты носителей, содержащих такие сведения, руководитель предприятия обязан незамедлительно проинформировать руководителя и службу безопасности (режимно-секретное подразделение) вышестоящего предприятия (если оно имеется) и организовать служебное расследование и розыск носителей сведений конфиденциального характера, а также принять меры по локализации возможного ущерба.

О факте разглашения сведений, составляющих государственную тайну, или утраты носителей, содержащих такие сведения еще дополнительно информируются органы безопасности[64]. Дальнейшие мероприятия по розыску утраченных носителей сведений конфиденциального характера, а также по выявлению обстоятельств разглашения сведений конфиденциального характера, и выявлению виновных лиц проводятся во взаимодействии с органами безопасности.

Для проведения служебного расследования руководитель предприятия не позднее следующего дня после обнаружения факта разглашения сведений конфиденциального характера, или утраты носителей, содержащих такие сведения, назначает комиссию из компетентных и не заинтересованных в исходе дела работников в составе не менее 3 человек (включая работника режимно-секретного подразделения), имеющих непосредственное отношение к данным сведениям и соответствующий допуск. При необходимости указанные работники освобождаются от исполнения своих служебных обязанностей на время проведения служебного расследования.

В работе комиссии могут принимать участие представители вышестоящего предприятия (если оно имеется).

Комиссия по ведению служебного расследования обязана:

---

[64] Федеральная служба безопасности функционирует на основании Федерального закона РФ от 3.04.1995 г. № 40-ФЗ "О федеральной службе безопасности" и Указа Президента РФ от 11.08.2003 г. № 960 "Вопросы Федеральной службы безопасности Российской Федерации".

- установить обстоятельства разглашения сведений конфиденциального характера, утраты носителей, содержащих такие сведения (время, место, способ и др.);

- вести розыск утраченных носителей сведений конфиденциального характера;

- установить лиц, виновных в разглашении сведений конфиденциального характера, утрате носителей, содержащих такие сведения;

- установить причины и условия, способствующие разглашению сведений конфиденциального характера, утрате носителей сведений, и выработать рекомендации по их устранению.

Члены комиссии по проведению служебного расследования имеют право:

- проводить осмотр помещений, участков местности, хранилищ, столов, шкафов, спецпортфелей и т.д., где могут находиться утраченные носители сведений конфиденциального характера;

- проверять полистно конфиденциальные документы, учетную документацию, отражающую их поступление и движение носителей сведений конфиденциального характера;

- опрашивать работников предприятия, допустивших разглашение конфиденциальных сведений, утрату носителей, содержащих такие сведения, а также других работников, могущих оказать содействие в установлении обстоятельств разглашения конфиденциальных сведений, утраты носителей, содержащих такие сведения, и получать от них письменные объяснения (показания);

- привлекать с разрешения руководителя предприятия других работников данного предприятия, не заинтересованных в исходе дела, для проведения отдельных действий в рамках служебного расследования.

При наличии достаточных оснований и по решению органа безопасности по факту разглашения сведений конфиденциального характера, или утраты носителей, содержащих такие сведения, возбуждается уголовное дело, и производятся необходимые следственные мероприятия. К ним относятся обыск помещений и изъятие документов и материалов.

Цель обыска как одного из предусмотренных законом следственных действий, возможного лишь после возбуждения уголовного дела, - сбор и фиксация доказательств, а также отыскание предметов и ценностей, которые могут быть конфискованы по приговору суда. В результате обыска могут быть обнаружены и изъяты лишь овеществленные объекты - орудия преступления, предметы, документы, иные носители информации (компьютерные диски, аудио-, видеозаписи и др.) и ценности.

В соответствии со статьей 182 "Основания и порядок производства обыска" Уголовно-процессуального кодекса РФ[65] обыск может быть проведен как на основании постановления следователя, не требующего чьей-либо санкции, так и на основании судебного решения, однако, если предполагается изымать предметы и материалы, составляющие государственную, или иную охраняемую законом тайну, то в соответствии со статьей 183 "Основания и порядок производства выемки" Уголовно-процессуального кодекса РФ обыск и выемка осуществляются только на основании постановления следователя и с санкции прокурора (см. приложение 7).

[65] Введен Федеральным законом РФ от 18.12.2001 г. № 174-ФЗ.

В производстве обыска обязательное участие принимают не менее двух понятых. Помимо названных лиц, в зависимости от обстоятельств дела и характера обыска, следователь вправе привлечь к участию в нем потерпевшего, свидетеля (если, например, необходимо опознать искомые предметы), специалиста, эксперта, переводчика, которые предупреждаются об ответственности, предусмотренной статьей 307 "Заведомо ложные показание, заключение эксперта, специалиста или неправильный перевод" и статьей 308 "Отказ свидетеля или потерпевшего от дачи показаний" Уголовного кодекса РФ, а также сотрудников органов, осуществляющих оперативно-розыскную деятельность[66]. Их участие обязательно оговаривается в протоколе следственного действия (см. приложение 8).

В протоколе должно быть указано, в каком месте и при каких обстоятельствах были обнаружены предметы или документы, выданы они добровольно или изъяты принудительно. Все изымаемые документы должны быть перечислены с точным указанием количества, наименования, даты составления, регистрационного номера, адресата, автора и т.п., количество страниц (листов).

Все изъятые при обыске (выемке) предметы и документы упаковываются и опечатываются на месте обыска, что удостоверяется подписями понятых.

Выемка информации в электронном виде, содержащейся на магнитных носителях, используемых в работе ПЭВМ возможна в двух вариантах: 1) изымается сам магнитный носитель (жесткий диск, гибкие магнитные диски, компактные оптические диски и иные съемные накопители); 2) изымается лишь относящаяся к делу (если ее возможно вычленить) информация. Изъятие такой информации может сопровождаться ее электронным копированием либо распечаткой на бумажных носителях. Все эти действия фиксируются в протоколе, изымаемый магнитный носитель опечатывается, а распечатанная на бумажном носителе информацию - заверяется подписями понятых и следователя, печатью следователя или предприятия, где произведен обыск (выемка).

Служебное расследование должно проводиться в предельно короткий срок, но не более месяца со дня обнаружения факта разглашения конфиденциальных сведений, утраты носителей, содержащих такие сведения.

В случае если утраченные носители сведений конфиденциального характера, не обнаружены, исчерпаны все возможные меры розыска, внесена ясность в обстоятельства их утраты и установлены виновные в этом лица, розыск может быть прекращен. Мотивированное заключение о прекращении розыска утверждается руководителем предприятия, назначившим комиссию по проведению служебного расследования, после чего оно рассматривается и утверждается руководителем вышестоящего предприятия (если оно имеется).

По окончании служебного расследования комиссия обязана представить руководителю организации на рассмотрение следующие документы:

- заключение о результатах проведенного служебного расследования;
- письменные объяснения лиц, которых опрашивали члены комиссии;
- акты проверок конфиденциальных документов и изделий, помещений, хранилищ, и т.п.;
- другие документы, имеющие отношение к служебному расследованию.

[66] Исчерпывающий перечень таких сотрудников представлен в статье 13 Федерального закона РФ от 12.08.1995 г. № 144-ФЗ "Об оперативно-розыскной деятельности".

Одновременно с комиссией по проведению служебного расследования руководителем предприятия создается комиссия по определению (уточнению) степени секретности разглашенных сведений (утраченных носителей сведений) в составе не менее 3 человек, не заинтересованных в исходе дела, имеющих непосредственное отношение к разглашенным сведениям (утраченным носителям) и соответствующий допуск.

В случае необходимости руководитель предприятия для участия в работе комиссии может привлекать работников из других предприятий (по согласованию с их руководителями), имеющих отношение к разглашенным сведениям (утраченным носителям), по которым дается заключение о степени их секретности.

Результаты работы комиссии по определению (уточнению) степени секретности разглашенных сведений (утраченных носителей) отражаются в мотивированном заключении, которое в предельно короткий срок, но не позднее 10 дней со дня создания комиссии представляется на утверждение руководителю предприятия.

По результатам работы комиссии руководитель предприятия принимает меры по локализации последствий разглашения сведений конфиденциального характера, утраты носителей, содержащих такие сведения.

Если комиссия по определению (уточнению) степени секретности разглашенных сведений (утраченных носителей) установит, что степень секретности разглашенных сведений или гриф секретности утраченных носителей сведений, не соответствует их содержанию, то заключение комиссии утверждается руководителем вышестоящего предприятия (если оно имеется) или руководителем органа государственной власти, наделенного полномочиями по распоряжению такими сведениями.

При необходимости по решению руководителя вышестоящего предприятия (если оно имеется) или руководителя органа государственной власти, наделенного полномочиями по распоряжению такими сведениями может быть проведено дополнительное служебное расследование или создана новая комиссия.

Степень секретности разглашенных сведений (утраченных носителей сведений), поступивших из другого предприятия, определяется (уточняется) комиссией этого предприятия либо комиссией вышестоящего предприятия (если оно имеется) и утверждается ее руководителем.

Заключение комиссии о степени секретности разглашенных сведений (утраченных носителей сведений) с приложением в случае необходимости копий материалов служебного расследования руководитель предприятия направляет руководителю вышестоящего предприятия (если оно имеется), а также в орган безопасности.

Один экземпляр заключения и материалы служебного расследования хранятся в службе безопасности (режимно-секретном подразделении).

Списание с учета утраченных носителей сведений конфиденциального характера, осуществляется на основании утвержденного руководителем предприятия акта о результатах служебного расследования.

На предприятиях ведется учет разглашенных конфиденциальных сведений (утраченных носителей) в "Журнале учета утрат секретных документов и фактов разглашения сведений конфиденциального характера".

14. ПРАВОВАЯ ЗАЩИТА КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

14.1. Уголовно-правовая защита сведений, составляющих коммерческую, налоговую или банковскую тайну

Характер и объем сведений, составляющих коммерческую, налоговую или банковскую тайну, определяются самим обладателем информации. Им же обеспечивается охрана ее конфиденциальности.

В соответствии с частью 1 статьи 183 Уголовного кодекса РФ (см. приложение 9) информация составляет служебную или коммерческую тайну в случае, когда информация имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам. Сведения, которые не могут составлять коммерческую тайну, определяются законом и иными нормативными актами[67].

Налоговую тайну в соответствии со статьей 102 Налогового Кодекса РФ составляют любые полученные налоговым органом, органами внутренних дел, органом государственного внебюджетного фонда и таможенным органом сведения о налогоплательщике, за исключением сведений: разглашенных налогоплательщиком самостоятельно или с его согласия; об идентификационном номере налогоплательщика; о нарушениях законодательства о налогах и сборах и мерах ответственности за эти нарушения; предоставляемых налоговым (таможенным) или правоохранительным органам других государств в соответствии с международными договорами (соглашениями), одной из сторон которых является Российская Федерация, о взаимном сотрудничестве между налоговыми, таможенными или правоохранительными органами (в части сведений, предоставленных этими органам).

К банковской тайне в соответствии со статьей 26 Федерального закона РФ "О банках и банковской деятельности[68]" относятся сведения об операциях, счетах и вкладах клиентов банка и его корреспондентов.

Статья 183 Уголовного кодекса РФ предусматривает три различных состава преступления, которые имеют один предмет посягательства - сведения, составляющие коммерческую, налоговую или банковскую тайну. В части 1 комментируемой статьи предусмотрена ответственность за собирание таких сведений путем похищения документов, подкупа или угроз, а равно иным незаконным способом в целях разглашения либо незаконного использования этих сведений. Наказуемы сами действия, предусмотренные в части 1 данной статьи, независимо от того, явились ли их результатом какие-либо последствия. Мотив преступления на квалификацию не влияет.

Субъектом преступления может быть любое лицо, достигшее 16-летнего возраста, не являющееся владельцем коммерческой, налоговой или банковской тайны и не допущенное к ней в установленном порядке.

Часть 2 комментируемой статьи предусматривает ответственность за незаконные разглашение или использование сведений, составляющих коммерче-

---

[67] В настоящее время такие сведения перечислены в постановлении Правительства РФ от 5.12.1991 г. № 35 "О передаче сведений, которые не могут составлять коммерческую тайну".

[68] Федеральный закон РФ от 2.12.1990 г. № 395-1 "О банках и банковской деятельности".

скую, налоговую или банковскую тайну, без согласия ее владельца, совершенные из корыстной или иной личной заинтересованности и причинившие крупный ущерб. Согласно части 2 комментируемой статьи субъектом преступления может быть любой работник организации или иные лица, которым сведения, составляющие коммерческую, налоговую или банковскую тайну, стали известны в связи с профессиональной или служебной деятельностью.

Часть 3 комментируемой статьи предусматривает ответственность за те же деяния, если в результате их совершения причинен крупный ущерб, а равно при наличии корыстной заинтересованности виновного. Обязательные элементы состава преступления - корыстная или иная личная заинтересованность виновного и крупный ущерб как последствие уголовно наказуемых действий.

В соответствии с частью 4 комментируемой статьи ответственность наступает за деяния, предусмотренные частью 2 или 3 этой статьи, повлекшие тяжкие последствия. Обязательное условие ответственности виновного лица по части 4 комментируемой статьи - наступление в результате указанных в части 2 или 3 этой статьи действий виновного лица тяжких последствий. Этот признак оценочный. Он может выражаться как в материальном, так и в ином ущербе.

При определении последствий преступления следует исходить как из стоимости оценки ущерба, так и из других существенных обстоятельств, например материального положения собственника или иного владельца имущества. Тяжкими последствиями могут быть признаны, например, экономическое разорение, дезорганизация работы коммерческого предприятия и т.п. Преступления, предусмотренные комментируемой статьей, совершаются умышленно.

14.2. Уголовно-правовая защита в сфере компьютерной информации

Информация - это сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления.

Под компьютерной информацией понимаются не сами сведения, а форма их представления в машиночитаемом виде, т.е. совокупность символов, зафиксированная в памяти компьютера либо на машинном носителе (дискете, оптическом, магнитооптическом диске, магнитной ленте либо ином материальном носителе).

Объективную сторону преступлений в сфере компьютерной информации составляет неправомерный доступ к охраняемой законом компьютерной информации (статья 272 Уголовного кодекса РФ, см. приложение 9), который всегда носит характер совершения определенных действий и может выражаться в проникновении в компьютерную систему путем:

- использования специальных технических или программных средств, позволяющих преодолеть установленные системы защиты;

- незаконного использования действующих паролей или кодов для проникновения в компьютер, либо совершении иных действий в целях проникновения в систему или сеть под видом законного пользователя;

- хищения носителей информации, при условии, что были приняты меры их охраны, если это деяние повлекло уничтожение или блокирование информации.

Неправомерным признается доступ к компьютерной информации лица, не обладающего правами на получение и работу с данной информацией либо компьютерной системой. Причем в отношении этой информации либо системы

должны приниматься специальные меры защиты, ограничивающие круг лиц, имеющих к ней доступ.

Под охраняемой законом информацией понимается информация, для которой в специальных законах установлен специальный режим ее правовой защиты, например - государственная, служебная и коммерческая тайна, персональные данные и т.д.

Состав данного преступления носит материальный характер и предполагает обязательное наступление одного из следующих последствий:

- уничтожение информации - приведение ее полностью либо в существенной части в непригодное для использования по назначению состояние;

- блокирование информации - обеспечение недоступности к ней, невозможности ее использования в результате запрещения дальнейшего выполнения последовательности команд либо выключения из работы какого-либо устройства, а равно выключения реакции какого-либо устройства ЭВМ, системы или сети ЭВМ при сохранении самой информации;

- модификация информации - внесение изменений в программы, базы данных, текстовую информацию, находящуюся на материальном носителе;

- копирование информации - перенос информации на другой материальный носитель, при сохранении неизмененной первоначальной информации;

- нарушение работы ЭВМ, системы ЭВМ или их сети, что может выразиться как в нарушении работы отдельных программ, баз данных, выдаче искаженной информации, так и в нештатном, т.е. не предусмотренном специальными инструкциями либо правилами, функционировании программно-аппаратных средств и периферийных устройств либо нарушении нормального функционирования сети.

Важным является установление причинной связи между несанкционированным доступом и наступлением последствий.

При этом следует учитывать, что неправомерный доступ может осуществляться к одной компьютерной информации, а вредоносные последствия наступать в отношении другой.

При функционировании сложных компьютерных систем возможны уничтожение, блокирование и нарушение работы ЭВМ в результате технических неисправностей или ошибок в программных средствах. В этом случае лицо, совершившее неправомерный доступ к компьютерной информации, не подлежит ответственности из-за отсутствия причинной связи между действиями и наступившими последствиями. Данное преступление считается оконченным в момент наступления предусмотренных в статье 272 Уголовного кодекса РФ последствий.

Субъективная сторона данного преступления характеризуется только прямым умыслом. В случае если в результате неправомерного доступа к системе ЭВМ, управляющей процессами, связанными с повышенной опасностью, например системе управления атомной станцией, в результате уничтожения, блокирования, модифицирования информации была нарушена работа реактора, что привело к тяжким последствиям, даже если наступление этих последствий не охватывалось умыслом лица, уголовная ответственность за такие последствия наступает в случае, если лицо предвидело возможность их наступления, но без достаточных к тому оснований самонадеянно рассчитывало на их предотвращение, или в случае, если лицо не предвидело, но должно было и могло предвидеть

возможность наступления этих последствий. В целом такое преступление признается совершенным умышленно.

Субъектами данного преступления в основном могут являться лица, имеющие опыт работы с компьютерной техникой, поэтому в силу профессиональных знаний они обязаны предвидеть возможные последствия уничтожения, блокирования, модификации информации либо нарушения работы ЭВМ, системы ЭВМ и их сети. По общему правилу субъектом преступления, предусмотренного комментируемой статьей, может быть лицо, достигшее 16-летнего возраста, однако часть 2 статьи 272 Уголовного кодекса РФ предусматривает наличие специального субъекта, совершившего данное преступление с использованием своего служебного положения, а равно имеющего доступ к ЭВМ, системе ЭВМ или их сети. Под доступом в данном случае понимается фактическая возможность использовать ЭВМ при отсутствии права на работу с защищенной информацией. Например, инженер по ремонту компьютерной техники имеет доступ к ЭВМ в силу своих служебных обязанностей, но вносить какие-либо изменения в информацию, находящуюся в памяти ЭВМ, не имеет права.

Создание, использование и распространение вредоносных программ для ЭВМ в соответствии со статьей 273 Уголовного кодекса РФ является также наказуемым деянием.

Под вредоносными программами понимаются программы, специально созданные для нарушения нормального функционирования компьютерных программ. Под нормальным функционированием понимается выполнение операций, для которых эти программы предназначены, что определено в документации на программу. В настоящее время самыми распространенными являются программы, предназначенные для сбора информации, и программы для несанкционированного доступа к ЭВМ либо другим программам.

Объективную сторону данного преступления составляет факт создания 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.

Под использованием программы понимается выпуск в свет, воспроизведение, распространение и иные действия по их введению в оборот. Использование может осуществляться путем записи программы в память ЭВМ, на материальный носитель, распространение по сетям либо путем иной передачи другим лицам. Данный состав является формальным и не требует наступления каких-либо последствий, уголовная ответственность возникает уже в результате создания программы, независимо от того, использовалась эта программа или нет. По смыслу статьи 273 Уголовного кодекса РФ наличие исходных текстов вирусных программ уже является основанием для привлечения к ответственности.

Формой совершения данного преступления может быть только действие, выраженное в виде создания вредоносных программ для ЭВМ, внесения изменений в уже существующие программы, а равно использование либо распространение таких программ. Распространение машинных носителей с такими программами полностью покрывается понятием "использование".

С субъективной стороны преступление, предусмотренное частью 1 статьи 273 Уголовного кодекса РФ, может быть совершено только с прямым умыслом,

так как в этой статье определено, что создание вредоносных программ заведомо для создателя программы должно привести к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ. Часть 2 комментируемой статьи в отличие от части 1 в качестве квалифицирующего признака предусматривает наступление тяжких последствий по неосторожности. Разработка вредоносных программ доступна только квалифицированным программистам, которые в силу своей профессиональной подготовки должны предвидеть возможные последствия использования этих программ. Субъектом данного преступления может быть любой гражданин, достигший 16 лет.

Компьютерные системы в настоящее время все больше влияют на нашу жизнь и выход из строя ЭВМ, систем ЭВМ или их сети может привести к катастрофическим последствиям, поэтому законодателем установлена уголовная ответственность за нарушение правил эксплуатации ЭВМ, систем ЭВМ или их сети (статья 274 Уголовного кодекса РФ).

Под охраняемой законом информацией понимается информация, для которой в специальных законах установлен специальный режим ее правовой защиты, например - государственная, служебная, коммерческая и банковская тайны, персональные данные и т.д.

Объективная сторона данного преступления состоит в нарушении правил эксплуатации ЭВМ, повлекшем уничтожение, блокирование или модификацию охраняемой законом информации ЭВМ при условии, что в результате этих действий был причинен существенный вред. Между фактом нарушения и наступившим существенным вредом должна быть установлена причинная связь и полностью доказано, что наступившие последствия являются результатом нарушения правил эксплуатации, а не программной ошибкой либо действиями, предусмотренными статьями 272 и 273 Уголовного кодекса РФ.

Понятие существенного вреда определяется самим потерпевшим и оценивается судом с учетом не только материального, но и морального ущерба, ущерба деловой репутации, вынужденных финансовых потерь и затрат на восстановление рабочего состояния ЭВМ, систем ЭВМ и их сети.

Субъективную сторону части 1 комментируемой статьи характеризует наличие умысла, направленного на нарушение правил эксплуатации ЭВМ. В случае наступления тяжких последствий ответственность по данной статье наступает только в случае неосторожных действий.

Умышленное нарушение правил эксплуатации ЭВМ, систем ЭВМ и их сети влечет уголовную ответственность в соответствии с наступившими последствиями, и нарушение правил эксплуатации в данном случае становится способом совершения преступления. Субъект данного преступления - специальный, это лицо, в силу должностных обязанностей имеющее доступ к ЭВМ, системе ЭВМ и их сети и обязанное соблюдать установленные для них правила эксплуатации.

14.3. Уголовно-правовая защита сведений, составляющих государственную тайну

Должностные лица и граждане, виновные в нарушении законодательства Российской Федерации о государственной тайне, несут уголовную, администра-

тивную, 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.

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

Нормы ответственности за правонарушения, связанные с государственной тайной, предусмотрены Уголовным кодексом РФ, который содержит статьи: статью 275 "Государственная измена", статью 276 "Шпионаж", статью 283 "Разглашение государственной тайны" и статью 284 "Утрата документов, содержащих государственную тайну" (см. приложение 9).

Федеральный закон РФ "О государственной гражданской службе Российской Федерации"[69] предусматривает возможность увольнения государственного служащего при однократном нарушении им своих обязанностей по защите государственной тайны.

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 Уголовного кодекса 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.

Сохранение конфиденциальности сведений, составляющих государственную тайну, является жизненно важным интересом отдельных лиц в тех, например, случаях, когда такая информация относится к ним самим или к их близким Заинтересованность в сохранении таких сведений объясняется тем, что их распространение создает угрозу законным интересам и безопасности указанных лиц, а нередко - их здоровью и самой жизни. В связи с этим законодательство Российской Федерации в ряде случае относит такого рода персональные данные к сведениям, составляющим государственную тайну.

Оконченным преступлением выдача государственной тайны признается с момента перехода сведений, ее составляющих, в адрес иностранного государства, иностранной организации либо их представителей. Представителями иностранного государства и иностранной организации являются их официальные лица (члены правительственных делегаций, сотрудники дипломатических представительств в России, сотрудники иностранных спецслужб, члены иностранных

[69] Федеральный закон РФ от 27.07.2004 г. № 79-ФЗ "О государственной гражданской службе Российской Федерации".

негосударственных организаций и т.д.), а также иные лица, выполняющие их поручения.

Могут иметь место стадии приготовления либо покушения на преступление (например, задержание виновного при попытке передать сведения указанным адресатам).

Уголовная ответственность предусмотрена за посягательство на государственную тайну независимо от того, к какой области (военной, экономической, научно-технической, внешнеполитической, внешнеэкономической, разведывательной, контрразведывательной или оперативно-розыскной 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

Государственная измена представляет собой акт предательства, т.е. оказание гражданином РФ помощи иностранному государству, иностранной организации или их представителям в осуществлении враждебной деятельности против Российской Федерации. Кроме общей формы измены в виде оказания помощи закон предусматривает ответственность за ее специальные формы - шпионаж, выдачу государственной тайны - если они направлены в ущерб внешней безопасности.

Как следует из текста статьи 275 и статьи 276 Уголовного кодекса РФ, устанавливающих уголовную ответственность за шпионаж, на государственную тайну посягает шпионаж, 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.

Измена в форме шпионажа по объективным признакам не отличается от шпионажа - самостоятельного преступления. Различаются они по субъекту: измену в форме шпионажа совершает гражданин России, а шпионаж по статье 276 - иностранный гражданин или лицо без гражданства.

Так же шпионажем признается передача или собирание по заданию иностранной разведки иных сведений, т.е. не составляющих государственную тайну, для использования в ущерб внешней безопасности Российской Федерации. Это не является посягательством на государственную тайну: он посягает на иную информацию.

Адресатами шпионажа выступают иностранные государства, иностранные организации и их представители. Под иностранными понимаются государства, на территорию которых не распространяется суверенитет Российской Федерации, независимо от того, в каких отношениях (враждебных, нейтральных, дружественных, союзных) находятся они с Россией.

Иностранные организации - это зарубежные объединения, партии, фирмы, концерны, ассоциации, а также международные, межнациональные, межправительственные, межгосударственные образования, в том числе и объединения иностранных государств, а равно филиалы таких иностранных организаций, действующие на территории Российской Федерации.

Представителями иностранных государств являются официальные сотрудники специальных служб, а также резиденты, агенты, осведомители, курьеры, связники этих служб, дипломатические и консульские представители этих государств, другие должностные лица, а также частные граждане, действующие от имени, по поручению или в интересах соответствующих иностранных государств. 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.

Передачей информации, составляющей государственную тайну, называется ее доведение до сведения иностранного государства, иностранной организации или их представителей независимо от способа сообщения. Передача незадокументированной информации осуществляется устно, письменно, другими способами. Документированная информация передается путем вручения (в том числе для временного пользования) документов, чертежей, фотографий, других материальных носителей информации, предметов, изделий. Она осуществляется лично, через посредников, по почте, по радио, по факсу, через компьютерную сеть, с использованием специальных средств связи, с помощью тайников, тайнописи, микрофотографии и т.п.

Собирание сведений, составляющих государственную тайну, заключается в завладении ими как с использованием различных технических средств, предназначенных для негласного получения информации, так и без их применения путем опроса (включая выведывание), наведение справок, сбора образцов для сравнительного исследования, закупки и обмена, исследования предметов и документов (включая фотографирование, копирование различными способами, временное заимствование носителя информации), наблюдения (визуального, слухового, с помощью приборов и др.), отождествления личности, обследования помещений, здании, сооружений, участков местности и транспортных средств, контроля почтовых отправлений, телеграфных и иных сообщений, прослушивания телефонных переговоров, снятия информации с технических каналов связи, вербовок лиц, осведомленных об интересующих субъекта сведениях, проведения экспериментов и т.п. При собирании сведений могут применяться обман, подкуп, шантаж и иные способы.

Похищение сведений заключается в противоправном изъятии у собственника, владельца или хранителя документальной информации, т.е. материальных носителей информации, содержащей государственную тайну, (документов, фотографий, кинопленок, кассет и иных носителей с аудио- и видеозаписями, перфокарт, дискет с компьютерной информацией, чертежей, схем, изделий, образцов вооружения, материалов и т.п.). При этом не имеет значения, законно или незаконно обладало указанной документальной информацией лицо, у которого она похищается. Похищение сведений может совершаться путем кражи, мошенничества, присвоения, грабежа, разбоя, вымогательства. При похищении, в отличие от собирания, сведения вместе с их носителями полностью изымаются из ведения их законного или незаконного обладателя (собственника, владельца или хранителя), так что их фактическим обладателем становится похититель.

Хранение сведений состоит в любых умышленных действиях, связанных с фактическим нахождением документированной информации, составляющей государственную тайну, у субъекта, независимо от продолжительности такого нахождения. При этом виновный сберегает подобную информацию, содержащуюся на материальном носителе (в документах, предметах, изделиях, веществах), которую он собрал, похитил, получил от третьих лиц, изготовил собственноручно (например, воспроизвел по памяти) либо завладел при других обстоятельствах Хранение сведений субъект может осуществлять при себе, в своем жилище, в специально подобранных местах (например, в тайниках), в камерах хранения, ломбардах, у других лиц, в том числе без их осведомления о характере хранящихся у них материалов, в памяти ЭВМ и т.п.

Уголовная ответственность за шпионаж, как и за остальные посягательства на государственную тайну, наступает с достижения виновным 16-летнего возраста.

Под разглашением сведений, составляющих государственную тайну (статья 283 Уголовного кодекса РФ), следует понимать противоправное предание огласке этих сведений, в результате чего они стали достоянием других лиц.

Постороннее лицо - это лицо, либо не имеющее доступа или допуска к государственной тайне, либо имеющее доступ или допуск, но не к тем сведениям, которые разглашены виновным. Разглашение окончено с момента, когда сведения, составляющие государственную тайну, стали известны постороннему лицу. Ответственность за разглашение несет только лицо, которому тайна была доверена или стала известна по службе или работе. Лицами, которым тайна доверена, следует считать лиц, имеющих допуск и доступ к государственной тайне.

К числу субъектов преступления относятся также лица, которым тайна специально не доверена, но может быть известна по роду деятельности, в силу специфики службы или работы (охранники, курьеры, водители, обслуживающий персонал закрытых учреждений).

Разглашение тайны совершается только умышленно, причем умысел может быть прямым или косвенным. При совершении преступления с прямым умыслом возникает вопрос об отграничении этого преступления от измены в форме выдачи государственной тайны и шпионажа. Отличие идет по характеру и содержанию умысла. При измене и шпионаже субъект осознает, что передает сведения иностранному государству, иностранной организации или их представителям, и желает передать государственную тайну указанным адресатам с целью проведения враждебной деятельности в ущерб внешней безопасности Российской Федерации. При разглашении тайны виновный осознает, что передает сведения постороннему лицу (не иностранному государству, организации или их представителям). Если же виновный передает тайну фактически указанным адресатам, но субъективно не осознает и не может осознавать характера адресата, то он также будет нести ответственность за разглашение тайны, а не за государственную измену.

Часть 2 статьи 283 Уголовного кодекса РФ устанавливает ответственность за разглашение государственной тайны, повлекшее по неосторожности тяжкие последствия. Тяжесть последствий определяется органами следствия и судом в зависимости от обстоятельств совершения преступления (важности разглашенных сведений, адресата, к которому они попали, использования этих сведений адресатом, ущерба от разглашения и т.д.). Субъектом преступления является ли-

цо, достигшее 16-летнего возраста, которому указанные сведения были доверены или стали известны по службе или работе.

В случае с утратой документов, составляющих государственную тайну (статья 284 Уголовного кодекса РФ) предметом преступления являются документы, т.е. письменные акты, содержащие сведения, являющиеся государственной тайной, имеющие соответствующие реквизиты (номер, подпись, печать, гриф секретности и т.д.) и зарегистрированные в соответствующих учреждениях и организациях.

Объективную сторону преступления характеризуют такие действия, как нарушение правил обращения с документами. Обязательным признаком объективной стороны являются последствия в виде утраты документа и наступления тяжких последствий, а также причинная связь между нарушением правил обращения с документами или предметами и утратой документов или предметов и тяжкими последствиями. Под утратой следует понимать выход документа или предмета из владения данного лица помимо воли этого лица, но в результате нарушения им установленных правил обращения с документами или предметами. Если утрата не повлекла тяжких последствий, состава данного преступления не будет. Преступление считается оконченным с момента утраты документа и наступления тяжких последствий.

Преступление совершается только лицами, имеющими допуск к государственной тайне (т.е. процедурно оформленное право на доступ к сведениям, составляющим государственную тайну). По отношению к последствиям вина может быть только неосторожной. В случае умышленного предоставления документа или предмета постороннему лицу речь должна идти о разглашении государственной тайны.

14.4. Административно-правовая защита информации с ограниченным доступом

Административная ответственность за нарушение порядка обращения с информацией ограниченного распространения в Кодексе об административных правонарушениях предусматривается по трем основным статьям (см. приложение 10).

В статье 13.12 "Нарушение правил защиты информации" объектом правонарушений, является порядок защиты информации. Объективная сторона предусмотренных частями 1 и 3 настоящей статьи правонарушений может заключаться как в действии, так и в бездействии, а правонарушений, предусмотренных частями 2 и 4, - только в действии.

Субъектами административных правонарушений, предусмотренных данной статьей, могут быть граждане, а также должностные лица и юридические лица. Вина в совершении данных правонарушений может быть как умышленной, так и неосторожной.

В статье 13.13 "Незаконная деятельность в области защиты информации" объектом правонарушений, является порядок осуществления деятельности в области защиты информации.

В соответствии с Федеральным законом РФ "Об информации, информационных технологиях и защите информации" предприятия, выполняющие работы в области проектирования, производства средств защиты информации (в том числе и информации, отнесенной к государственной тайне), должны иметь ли-

цензии на данные виды деятельности. Объективная сторона предусмотренных настоящей статьей правонарушений может заключаться только в действии.

Субъектами административных правонарушений, предусмотренных данной статьей, могут быть граждане, а также должностные лица и юридические лица. Вина в совершении данных правонарушений может быть как умышленной, так и неосторожной.

В статье 13.14 "Разглашение информации с ограниченным доступом" объектом правонарушения, предусмотренного данной статьей, является порядок получения информации с ограниченным доступом.

Объективная сторона данного правонарушения состоит в действии, представляющем собой 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. Документированная информация с ограниченным доступом по условиям ее правового режима подразделяется на информацию, отнесенную к государственной тайне, и конфиденциальную.

Отнесение информации к государственной тайне осуществляется в соответствии с Законом РФ "О государственной тайне". Отнесение информации к конфиденциальной осуществляется в порядке, установленном отраслевым законодательством РФ (гражданским, административным и т.д.). Субъектами административного правонарушения, предусмотренного данной статьей, могут быть граждане, а также должностные лица. Вина в совершении данного правонарушения может быть как умышленной, так и неосторожной.

14.5. Гражданско-правовая защита служебной и коммерческой тайны

В Гражданском кодексе РФ определено, что для защиты своих гражданских прав можно пользоваться только способами, которые предусмотрены в законе. Непосредственно в статье 12 Гражданского кодекса РФ (см. приложение 11) перечислены способы, наиболее часто встречающиеся в судебной и хозяйственной практике. Но этот перечень не исчерпывающий.

Применить те или иные способы защиты могут сами управомоченные и обязанные лица, суды, а также соответствующие органы в административном порядке (статья 10 Гражданского кодекса РФ). Некоторые способы вправе применить или только суды, или только управомоченные лица.

К первым можно отнести признание оспоримой сделки недействительной и применение последствий ее недействительности; неприменение судом акта государственного органа или органа местного самоуправления, противоречащего закону.

Для защиты гражданских прав возможно использовать возмещение убытков) либо признание права на вещь и присуждение к ее возврату в натуре; возмещение убытков и взыскание неустойки; признание акта органа государственного управления недействительным и возмещение убытков, причиненных изданием этого акта, и т.п.).

Признание прав как способ защиты может применяться в сочетании с другими способами, например признание права и восстановление положения, существовавшего до нарушения права, а также пресечение действий, нарушающих право.

Компенсация морального вреда установлена для защиты нематериальных благ (личных неимущественных прав) граждан (статьи 151-152 Гражданского кодекса РФ) и в других предусмотренных законом случаях (статьи 1099-1101 Гражданского кодекса РФ).

В статье 139 "Служебная и коммерческая тайна" Гражданского кодекса РФ (см. приложение 11) субъекты гражданского права могут в своих интересах ограничивать доступ других лиц к известной им информации. Поэтому в отличие от государственной тайны состав сведений, которые составляют служебную или коммерческую тайну, определяется не нормативными актами, а самими обладателями информации. Виды информации, составляющие служебную и коммерческую тайну, определяются внутренними (локальными) нормативными актами организаций, гражданско-правовыми и трудовыми договорами.

Лишь в некоторых случаях, когда деятельность предприятия связана с использованием информации, охраняемой в интересах других лиц (не обладателя) или силу иных норм права, например конституционных прав граждан на тайну личной жизни, законодатель изначально определяет, что сведения, которыми обладает организация, относятся к коммерческой тайне.

В статье практически не разделяются понятия служебной и коммерческой тайны и предусматривается одинаковое регулирование для обоих видов тайны, что связано с невозможностью четкого разделения регулируемых отношений. Информация, являющаяся коммерческой тайной, может стать служебной тайной и наоборот. Состав информации, являющейся коммерческой и служебной тайной, также часто совпадает по составу с другими видами конфиденциальной информации, в том числе государственной, налоговой, банковской тайной.

Для признания информации служебной или коммерческой тайной и соответственно для ее правовой охраны закон называет следующие обязательные условия:

1) наличие у информации действительной или потенциальной коммерческой ценности;

2) неизвестность информации третьим лицам;

3) отсутствие свободного доступа к информации на законном основании;

4) обладатель информации принимает меры к охране конфиденциальности информации, среди них можно выделить три основных вида:

- организационные, заключающиеся в определении информации как служебной и коммерческой тайны и доведении этого до тех, кто находится в непосредственном контакте с информацией (работники, контрагенты);

- юридические, заключающиеся в установлении обязанности в договорах (трудовых и гражданско-правовых) контрагентов и работников соблюдать конфиденциальность, а именно: не разглашать информацию, соблюдать технические меры работы с информацией. Для договоров подряда такая обязанность установлена в статье 727 второй части Гражданского кодекса РФ;

- технические, препятствующие разглашению работниками и контрагентами (активные) и затрудняющие доступ третьих лиц (пассивные).

Среди способов защиты информации, предусмотренных действующим законодательством, можно назвать следующие:

- специальный порядок получения сведений от их обладателей, в том числе ограничение круга лиц, уполномоченных получать такие сведения (например, часть 3 статьи 183 Уголовно-процессуального кодекса РФ);

- особую процедуру работы с таким сведениями (так, пункт 2 статьи 11 Арбитражного процессуального кодекса РФ[70] и пункт 2. статьи 10 Гражданско-процессуального кодекса РФ[71] предусматривают возможность проведения закрытого судебного заседания по ходатайству лица, участвующего в деле и ссылающегося на необходимость сохранения тайны);

- ответственность государственных органов и должностных лиц за разглашение коммерческой и служебной тайны.

Необходимо отметить, что статья 139 Гражданского кодекса РФ устанавливает ответственность в виде возмещения убытков не только за незаконное разглашение, но и за незаконное получение информации, составляющей служебную и коммерческую тайну.

14.6. Дисциплинарная ответственность за разглашение и (или) утрату конфиденциальных сведений

За разглашение государственной, коммерческой, служебной или иной охраняемой законом тайны трудовым законодательством установлена дисциплинарная ответственность (см. приложение 12).

В статье 81 "Расторжение трудового договора по инициативе работодателя" Трудового кодекса РФ установлено 13 оснований увольнения работников по инициативе работодателя.

Пункт 6 статьи 81 Трудового кодекса РФ предусматривает 5 грубых нарушений работником своих трудовых обязанностей, и каждое из них является самостоятельным основанием увольнения даже при отсутствии у него дисциплинарных взысканий. Все они - крайние меры дисциплинарного взыскания. Поэтому по всем пяти подпунктам пункта 6 статьи 81 Трудового кодекса РФ должны быть соблюдены сроки и правила наложения дисциплинарных взысканий (статьи 192 и 193 Трудового кодекса РФ).

Подпунктом "в" пункта 6 статьи 81 Трудового кодекса РФ закреплено основание увольнения, отнесенное к грубым нарушениям, - разглашение охраняемой законом тайны (государственной, коммерческой, служебной и иной), ставшей известной работнику в связи с исполнением им трудовых обязанностей. Работодатель может уволить работника за однократный такой проступок. Так как абсолютное большинство работников не знают, что относится к коммерческой и служебной, а тем более иной тайне, этим основанием увольнения работодатели могут злоупотреблять. Поэтому по данному вопросу требуются обязательно дополнительные разъяснения, например, все ли работники предприятия отвечают за коммерческую или служебную тайну, ее разглашение или только те, в трудовых договорах которых указано соответствующее условие, является ли охраняемой законом тайной то, что указано в уставе предприятия, и т.д.

Пунктом 11 статьи 81 Трудового кодекса РФ предусмотрено общее основание увольнения - это представление работником работодателю подложных документов или заведомо ложных сведений при заключении трудового договора. Конечно, подложность документов должна быть обоснована соответствующей их криминалистической экспертизой и другими доказательствами. Что касается заведомо ложных сведений, то, такие сведения должны влиять на работу.

---

[70] Введен Федеральным законом РФ от 24.07.2002 г. № 95-ФЗ.

[71] Введен Федеральным законом РФ от 14.11.2002 г. № 138-ФЗ.

Пункт 12 статьи 81 Трудового кодекса РФ закрепил основание для увольнения - прекращение допуска к государственной тайне, если выполняемая работа требует допуска.

Дисциплинарная ответственность работников является самостоятельным видом юридической ответственности. К дисциплинарной ответственности могут привлекаться работники, совершившие дисциплинарный проступок. Следовательно, основанием такой ответственности всегда служит дисциплинарный проступок, совершенный конкретным работником. Дисциплинарным проступком признается противоправное, виновное неисполнение или ненадлежащее исполнение работником своих трудовых обязанностей.

Как и любое другое правонарушение, дисциплинарный проступок обладает совокупностью признаков: субъект, субъективная сторона, объект, объективная сторона. Субъектом дисциплинарного проступка может быть гражданин, состоящий в трудовых правоотношениях с конкретной организацией и нарушающий трудовую дисциплину. Субъективной стороной дисциплинарного проступка выступает вина со стороны работника. Она может быть в форме умысла или по неосторожности. Объект дисциплинарного проступка - внутренний трудовой распорядок конкретной организации. Объективной стороной здесь выступают вредные последствия и прямая связь между ними и действием (бездействием) правонарушителя.

В соответствии с заключенным трудовым договором работодатель вправе требовать от работника выполнения трудовых обязанностей. Согласно статьи 192 "Дисциплинарные взыскания" Трудового кодекса РФ работодатель имеет право, но не обязан привлекать к дисциплинарной ответственности работника, совершившего дисциплинарный проступок. В части 1 статьи 192 Трудового кодекса РФ установлены меры дисциплинарных взысканий, налагаемые на нарушителей трудовой дисциплины. Работодатель вправе применить одну из указанных мер.

Самой строгой мерой дисциплинарного взыскания является увольнение. Оно возможно в следующих случаях: неоднократное неисполнение работником без уважительных причин трудовых обязанностей, если он имеет дисциплинарное взыскание; разглашение охраняемой законом тайны (государственной, коммерческой, служебной и иной), ставшей известной работнику в связи с исполнением им трудовых обязанностей и т.п.

Существуют два вида дисциплинарной ответственности: общая, предусмотренная Трудовым кодексом РФ, и специальная, которую несут работники в соответствии с уставами и положениями о дисциплине.

При общей дисциплинарной ответственности перечень мер взыскания, предусмотренный статьей 192 Трудового кодекса РФ, является исчерпывающим. Сами предприятия никаких дополнительных дисциплинарных взысканий устанавливать не могут, хотя на практике иногда применяются такие санкции, как штрафы, лишение разного рода надбавок, выговор с предупреждением и другие, которые нельзя признать законными.

Специальную дисциплинарную ответственность несут работники, на которых распространяются уставы и положения о дисциплине. В этих актах, как уже отмечалось, могут предусматриваться и более строгие меры взыскания, отличающиеся от тех, которые возлагаются на работников при общей дисципли-

нарной ответственности, хотя и при специальной применяются меры, в том числе перечисленные в статье 192 Трудового кодекса РФ.

Специальную дисциплинарную ответственность несут государственные служащие на основе Федерального закона РФ "О государственной гражданской службе в Российской Федерации".

В соответствии с этим Законом на государственного служащего кроме указанных в статье 192 Трудового кодекса РФ может быть наложено предупреждение о неполном должностном соответствии. Кроме того, государственный служащий, допустивший должностной проступок, может быть освобожден от замещаемой должности гражданской службы.

Положения и уставы о дисциплине обязательны для всех работников, которые подпадают под их действие. Сами работодатели не имеют права вносить в них дополнения и изменения. Одним из отличий этих актов, поэтому является наличие в них более строгих, чем для всех остальных работников, мер взыскания.

При применении меры взыскания администрацией при общей дисциплинарной ответственности должны учитываться степень тяжести проступка, вред, причиненный им, обстоятельства, при которых он совершен, и общая характеристика лица, совершившего дисциплинарный проступок. При этом совсем не обязательно сохранять последовательность взысканий, указанных в статье 192 Трудового кодекса РФ. Решение о применении меры взыскания выносит работодатель, который может и не воспользоваться предоставленным ему Трудовым кодексом РФ правом и ограничиться устным замечанием, беседой и т.п.

В соответствии с частью 1 статьи 193 Трудового кодекса РФ до применения дисциплинарного взыскания от работника должно быть затребовано письменное объяснение причин проступка. Его отказ дать такое объяснение не является препятствием для дисциплинарного взыскания. Требование от работника представления объяснения - одна из гарантий того, что наложение взыскания будет правомерно. Отсутствие объяснения должно быть подтверждено соответствующим актом об отказе работника дать объяснение.

Днем обнаружения дисциплинарного проступка считается день, когда должностному лицу, которому подчинен работник, стало известно о проступке, независимо от того, наделено это лицо правом наложения взысканий или нет. В месячный срок для наложения взыскания не засчитывается время болезни работника или нахождения его в отпуске (очередном, учебном, оплачиваемом или без сохранения содержания). Отсутствие на работе по другим основаниям не прерывает течение указанного срока. Однако на практике время прогула, когда работник мог не знать о наложении взыскания, обычно не включается в данный месячный срок, и последний начинает исчисляться с момента выхода работника на работу. Но в любом случае взыскание не может быть наложено по истечении шести месяцев со дня совершения проступка, независимо от времени его обнаружения. Исключение составляют проступки, которые обнаружены по результатам ревизий и проверок финансово-хозяйственной деятельности или аудиторской проверки. В этом случае срок удлиняется до двух лет со дня совершения проступка. В указанные сроки не включается время производства по уголовному делу.

Часть 5 статьи 193 Трудового кодекса РФ не допускает применения нескольких дисциплинарных взысканий за один проступок. Однако при причине-

нии ущерба работником возможно сочетание дисциплинарных и материальных санкций, поскольку дисциплинарная и материальная ответственность имеют разное целевое назначение и могут совмещаться.

Приказ (распоряжение) о применении дисциплинарного взыскания объявляется работнику под расписку. В случае его отказа расписаться составляется соответствующий акт, который подписывают свидетельствующие этот факт лица. Наложенное дисциплинарное взыскание может быть обжаловано работником в органы по рассмотрению индивидуальных споров (комиссию по трудовым спорам и суд) или в государственную инспекцию труда.

В соответствии со статьей 194 Трудового кодекса РФ дисциплинарное взыскание, наложенное на работника, сохраняет свою силу в течение года со дня его применения. Если в течение этого года работник не будет, подвергнут новому дисциплинарному взысканию, он считается не имеющим дисциплинарного взыскания. В этом случае по прошествии года старое взыскание теряет силу, и это не требует никакого нового приказа (распоряжения). Работодатель может снять наложенное на работника взыскание досрочно, если тот не совершил новых нарушений трудовой дисциплины и проявил себя позитивно. Для досрочного снятия взыскания необходимо издание соответствующего приказа (распоряжения) работодателя.

14.7. Материальная ответственность за разглашение и (или) утрату конфиденциальных сведений

Трудовым кодексом РФ предусмотрена материальная ответственность работника за причиненный ущерб работодателю и наоборот, работодателем работнику (см. приложение 12).

Так, в статье 232 "Обязанность стороны трудового договора возместить ущерб, причиненный ею другой стороне этого договора" Трудового кодекса РФ указано, что к трудовому договору могут быть по соглашению сторон разработаны приложения в форме письменного соглашения о материальной ответственности. Таким же приложением к трудовому договору может выступать должностная инструкция. Даже с согласия работника материальная ответственность работника не может быть выше установленной Трудовым кодексом РФ. Соответственно материальная ответственность не может быть ниже установленной Трудовым кодексом РФ.

При хищении, недостаче, умышленном уничтожении или умышленной порче материальных ценностей ущерб рассчитывается по розничным ценам, а в случаях, когда розничные цены на материальные ценности ниже оптовых цен, - по оптовым ценам.

Законодательством может быть установлен особый порядок определения размера подлежащего возмещению ущерба (в том числе в кратном исчислении), причиненного предприятию хищением, умышленной порчей, недостачей или утратой отдельных видов имущества и других ценностей (в том числе и конфиденциальной информации) в тех случаях, когда фактический размер ущерба превышает его номинальный размер.

Размер возмещаемого ущерба, причиненного по вине нескольких работников, определяется для каждого из них с учетом степени вины, вида и предела материальной ответственности. Материальная ответственность сторон трудового договора заключается в обязанности одной из сторон трудового правоотношения

возместить имущественный ущерб, причиненный ею другой стороне в результате ненадлежащего исполнения своих трудовых обязанностей.

Материальная ответственность - самостоятельный вид ответственности, отличающийся от ответственности, установленной по нормам гражданского права. Субъектом материальной ответственности может быть только работник, находящийся в трудовых правоотношениях с работодателем.

В соответствии со статьей 233 "Условия наступления материальной ответственности стороны трудового договора" Трудового кодекса РФ условиями наступления материальной ответственности сторон трудового договора являются следующие юридические факты:

1) причиненный ущерб;

2) виновное поведение;

3) противоправное поведение;

4) причинная связь между виновным поведением и ущербом.

Причиненный ущерб - утрата, хищение, уничтожение, ухудшение, понижение ценности имущества и возникновение необходимости для предприятия произвести затраты на восстановление, приобретение имущества или иных ценностей либо сделать излишние выплаты.

Противоправное поведение - это такое поведение (действия, бездействие), при котором работник не исполняет свои обязанности, возложенные на него Трудовым кодексом РФ (статьей 21), трудовым договором, должностной инструкцией, правилами внутреннего трудового распорядка, коллективным договором.

Причинная связь - действие или бездействие работника должно быть причиной наступления ущерба. Действия работника могут быть как причиной ущерба, так и создавать условия для его возникновения.

Вина работника заключается в том, что он совершил противоправное действие (бездействие) умышленно или по неосторожности.

Умышленные действия характеризуются тем, что работник предвидел вредные последствия своего поведения (наступление ущерба) и желал или допускал их наступление.

Неосторожность работника характеризуется недостаточной предусмотрительностью работника. Работник либо не предвидел наступление последствия - ущерба, либо легкомысленно надеялся его предотвратить. Это разновидность небрежности в работе.

Согласно статьи 21 Трудового кодекса РФ работник обязан бережно относиться к имуществу работодателя и других работников. Если он причиняет ущерб, то на него возлагается материальная ответственность. Ущербом считается вред, причиненный имуществу работодателя.

В соответствии со статьей 238 "Материальная ответственность работника за ущерб, причиненный работодателю" Трудового кодекса РФ в процессе проведения расследования происшествия и определения пределов материальной ответственности работника необходимо собрать следующие доказательства, подтверждающие:

1) вину работника;

2) наличие прямого действительного ущерба;

3) противоправность действия (бездействие) работника;

4) причинную связь между его действием (бездействием) и ущербом, с тем чтобы с учетом этих данных, а также обстоятельств, от которых зависит правильное определение вида и пределов материальной ответственности, разрешить возникший спор по существу.

В случае если ущерб причинен умышленными действиями работника, в том числе, когда работник не желал, но сознательно допускал возможность возникновения ущерба, наступает материальная ответственность в полном размере (статья 242 "Полная материальная ответственность работника", статья 243 "Случаи полной материальной ответственности" Трудового кодекса РФ).

Полная материальная ответственность работника по предусмотренным статьей 243 Трудового кодекса РФ основаниям наступает и в случае недостачи указанных ценностей независимо от формы его вины.

Если же при рассмотрении дела будет установлено, что ущерб причинен в результате небрежности работника, он может быть привлечен к ограниченной материальной ответственности в пределах своего среднего месячного заработка (статья 241 "пределы материальной ответственности работника" Трудового кодекса РФ).

Статьей 239 "Обстоятельства, исключающие материальную ответственность работника" Трудового кодекса РФ определены следующие обстоятельства, исключающие ответственность работника за разглашение, уничтожение, утрату конфиденциальной информации:

- действия непреодолимой силы - чрезвычайные, неотвратимые обстоятельства, объективные и абсолютные, т.е. это действие факторов, ставших препятствием выполнения обязанности работника. Эти препятствия касаются не только причинителя вреда, но распространяются на всех. Работник при непреодолимой силе не может исполнить свою обязанность по обеспечению сохранности вверенного ему имущества. Видами непреодолимой силы являются стихийные бедствия или иные обстоятельства, которые можно предусмотреть, но невозможно предотвратить;

- крайняя необходимость - состояние, деятельность, в результате которой работник устраняет опасность, угрожающую интересам личности, государства, общественным интересам, работодателю, другим гражданам. Эти действия причиняют вред работодателю, но работник освобождается от ответственности, так как вред не мог быть предотвращен другим способом и причиненный вред менее предотвращенного (к этим условиям могут относиться: выдача конфиденциальной информации по требованию органов государственной власти, экстренное уничтожение информации и т.п.);

- неисполнение работодателем обязанности по обеспечению надлежащих условий для хранения имущества, вверенного работнику, - бездействие работодателя (невыполнение обязанности), в результате которого работник не смог выполнить свои обязанности по обеспечению сохранности доверенной ему ценности. Например, работник сообщил работодателю о том, что в помещении, в котором находятся вверенные ему ценности (конфиденциальная информация), сломался замок, либо неисправна сигнализация. До конца рабочего дня работодатель не обеспечил ремонт замка, а на другой день часть ценностей (конфиденциальной информации) пропала. В данной ситуации работник освобождается от материальной ответственности.

В соответствии со статьей 240 "Право работодателя на отказ от взыскания ущерба с работника" Трудового кодекса РФ право работодателя на отказ от взыскания с виновного работника ущерба является абсолютным, т.е. не ограничено никакими условиями. Работодатель решает самостоятельно взыскивать ущерб, полностью отказаться от взыскания или взыскать его частично. В то же время работодатель может установить перечень обстоятельств в нормативном правовом акте предприятия, например в коллективном договоре, при наступлении которых работодатель не будет взыскивать причиненный ущерб. К таким обстоятельствам можно отнести: отсутствие умысла работника на причинение ущерба; работник рисковал в интересах предприятия, его действия - это нормальный производственный риск и т.д.

По каждому факту хищений, недостач и порчи материальных ценностей проводится служебное расследование. Основанием для проведения служебного расследования являются задержание с поличным, результаты инвентаризаций, ревизий, данные, содержащиеся в материалах претензионных, арбитражных и судебных дел, в заявлениях и письмах граждан.

В соответствии со статьей 248 "Порядок взыскания ущерба" Трудового кодекса РФ взыскание с виновного работника суммы причиненного ущерба, не превышающей среднего месячного заработка, производится по распоряжению работодателя. Распоряжение может быть сделано не позднее одного месяца со дня окончательного установления работодателем размера причиненного работником ущерба.

В судебном порядке происходит взыскание при наличии следующих юридических фактов:

если месячный срок истек;

работник не согласен добровольно возместить причиненный работодателю ущерб;

сумма причиненного ущерба, подлежащая взысканию с работника, превышает его средний месячный заработок.

Размер причиненного ущерба определяется по фактическим потерям, на основании данных бухгалтерского учета, исходя из балансовой стоимости материальных ценностей за вычетом износа по установленным нормам.

Возмещение ущерба производится независимо от привлечения работника к дисциплинарной, административной или уголовной ответственности за действие (бездействие), которым причинен ущерб предприятию.

ЗАКЛЮЧЕНИЕ

В учебном пособии подробно раскрыты основные направления работы по организационно-правовой защите информации на предприятии, являющиеся сегодня наиболее актуальными. Для этих направлений представлены основные задачи должностных лиц и функции структурных подразделений предприятия, последовательность и алгоритм решения задач по организационно-правовой защите информации с учетом положений нормативно-методических документов и специфики деятельности предприятия. По каждому из этих направлений сделаны выводы о наиболее эффективном решении задач при организации работы по защите конфиденциальной информации.

Однако, наряду с изложенными направлениями в целях решения задач по комплексной защите информации необходимо выделять и другие направления, определяющие вопросы обеспечения информационной безопасности исходя из специфики повседневной деятельности предприятия и задач, решаемых им при проведении видов работ, предусмотренных уставом.

Сегодня роль и место организационной составляющей в общей системе защиты конфиденциальной информации предприятия трудно переоценить. Организационная защита информации призвана на основе установленных норм и правил защиты информации с учетом совокупности сил и средств, используемых способов и методов защиты информации, определить наиболее эффективные меры, направленные на сохранение конфиденциальности информации и исключение возможных каналов ее утечки.

При решении задач организационно-правовой защиты информации на предприятии важно обеспечить комплексный подход к проблеме защиты информации, а также полный охват направлений и видов деятельности предприятия, связанных с конфиденциальной информацией.

Особое внимание в работе по защите информации на предприятии должно быть уделено человеческому фактору как основе успешного решения поставленных в данной области задач, так как четко сформулированная и реализованная концепция работы с персоналом предприятия позволит исключить возникновение негативных факторов, влияющих на уровень защиты информации в целом.

Успешное решение рассмотренных в учебном пособии, а также многих других вопросов в области комплексной защиты информации - важный шаг на пути достижения цели - сохранении конфиденциальности защищаемых предприятием сведений о его деятельности.

ПРИЛОЖЕНИЕ 1

Федеральный Закон Российской Федерации "О персональных данных" (от 27 июля 2006 г. № 152-ФЗ) (извлечения)

Статья 3. Основные понятия, используемые в настоящем Федеральном законе.

В целях настоящего Федерального закона используются следующие основные понятия:

1) персональные данные - любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация;

12) общедоступные персональные данные - персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.

Статья 6. Условия обработки персональных данных.

1. Обработка персональных данных может осуществляться оператором с согласия субъектов персональных данных, за исключением случаев, предусмотренных частью 2 настоящей статьи.

2. Согласия субъекта персональных данных, предусмотренного частью 1 настоящей статьи, не требуется в следующих случаях:

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

2) обработка персональных данных осуществляется в целях исполнения договора, одной из сторон которого является субъект персональных данных;

3) обработка персональных данных осуществляется для статистических или иных научных целей при условии обязательного обезличивания персональных данных;

4) обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно;

5) обработка персональных данных необходима для доставки почтовых отправлений организациями почтовой связи, для осуществления операторами электросвязи расчетов с пользователями услуг связи за оказанные услуги связи, а также для рассмотрения претензий пользователей услугами связи;

6) обработка персональных данных осуществляется в целях профессиональной деятельности журналиста либо в целях научной, литературной или иной творческой деятельности при условии, что при этом не нарушаются права и свободы субъекта персональных данных;

7) осуществляется обработка персональных данных, подлежащих опубликованию в соответствии с федеральными законами, в том числе персональных данных лиц, замещающих государственные должности, должности государственной гражданской службы, персональных данных кандидатов на выборные государственные или муниципальные должности.

3. Особенности обработки специальных категорий персональных данных, а также биометрических персональных данных устанавливаются соответственно статьями 10 и 11 настоящего Федерального закона.

4. В случае если оператор на основании договора поручает обработку персональных данных другому лицу, существенным условием договора является обязанность обеспечения указанным лицом конфиденциальности персональных данных и безопасности персональных данных при их обработке.

Статья 7. Конфиденциальность персональных данных.

1. Операторами и третьими лицами, получающими доступ к персональным данным, должна обеспечиваться конфиденциальность таких данных, за исключением случаев, предусмотренных частью 2 настоящей статьи.

2. Обеспечения конфиденциальности персональных данных не требуется:

1) в случае обезличивания персональных данных;

2) в отношении общедоступных персональных данных.

Статья 8. 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, предоставленные субъектом персональных данных.

2. Сведения о субъекте персональных данных могут быть в любое время исключены из общедоступных источников персональных данных по требованию субъекта персональных данных либо по решению суда или иных уполномоченных государственных органов.

Статья 9. Согласие субъекта персональных данных на обработку своих персональных данных.

1. Субъект персональных данных принимает решение о предоставлении своих персональных данных и дает согласие на их обработку своей волей и в своем интересе, за исключением случаев, предусмотренных частью 2 настоящей статьи. Согласие на обработку персональных данных может быть отозвано субъектом персональных данных.

2. Настоящим Федеральным законом и другими федеральными законами предусматриваются случаи обязательного предоставления субъектом персональных данных своих персональных данных в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства.

3. Обязанность предоставить доказательство получения согласия субъекта персональных данных на обработку его персональных данных, а в случае обработки общедоступных персональных данных обязанность доказывания того, что обрабатываемые персональные данные являются общедоступными, возлагается на оператора.

4. В случаях, предусмотренных настоящим Федеральным законом, обработка персональных данных осуществляется только с согласия в письменной форме субъекта персональных данных. Письменное согласие субъекта персональных данных, на обработку своих персональных данных должно включать в себя:

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

3) цель обработки персональных данных;

4) перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;

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

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

5. Для обработки персональных данных, содержащихся в согласии в письменной форме субъекта на обработку его персональных данных, дополнительного согласия не требуется.

6. В случае недееспособности субъекта персональных данных согласие на обработку его персональных данных дает в письменной форме законный представитель субъекта персональных данных.

7. В случае смерти субъекта персональных данных согласие на обработку его персональных данных дают в письменной форме наследники субъекта персональных данных, если такое согласие не было дано субъектом персональных данных при его жизни.

Статья 10. Специальные категории персональных данных.

1. Обработка специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни, не допускается, за исключением случаев, предусмотренных частью 2 настоящей статьи.

2. Обработка указанных в части 1 настоящей статьи специальных категорий персональных данных допускается в случаях, если:

1) субъект персональных данных дал согласие в письменной форме на обработку своих персональных данных;

2) персональные данные являются общедоступными;

3) персональные данные относятся к состоянию здоровья субъекта персональных данных и их обработка необходима для защиты его жизни, здоровья или иных жизненно важных интересов либо жизни, здоровья или иных жизненно важных интересов других лиц, и получение согласия субъекта персональных данных невозможно;

4) 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 ме-

дицинской деятельностью и обязанным в соответствии с законодательством Российской Федерации сохранять врачебную тайну;

5) 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;

6) обработка персональных данных необходима в связи с осуществлением правосудия;

7) обработка персональных данных осуществляется в соответствии с законодательством Российской Федерации о безопасности, об оперативно-розыскной деятельности, а также в соответствии с уголовно-исполнительным законодательством Российской Федерации.

3. 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.

4. Обработка специальных категорий персональных данных, осуществлявшаяся в случаях, предусмотренных частями 2 и 3 настоящей статьи, должна быть незамедлительно прекращена, если устранены причины, вследствие которых осуществлялась обработка.

Статья 11. Биометрические персональные данные.

1. Сведения, которые характеризуют физиологические особенности человека и на основе которых можно установить его личность (биометрические персональные данные), могут обрабатываться только при наличии согласия в письменной форме субъекта персональных данных, за исключением случаев, предусмотренных частью 2 настоящей статьи.

2. Обработка биометрических персональных данных может осуществляться без согласия субъекта персональных данных в связи с осуществлением правосудия, а также в случаях, предусмотренных законодательством Российской Федерации о безопасности, законодательством Российской Федерации об оперативно-розыскной деятельности, законодательством Российской Федерации о государственной службе, уголовно-исполнительным законодательством Российской Федерации, законодательством Российской Федерации о порядке выезда из Российской Федерации и въезда в Российскую Федерацию.

Статья 14. Право субъекта персональных данных на доступ к своим персональным данным.

1. Субъект персональных данных имеет право на получение сведений об операторе, о месте его нахождения, о наличии у оператора персональных данных, относящихся к соответствующему субъекту персональных данных, а также на ознакомление с такими персональными данными, за исключением случаев, предусмотренных частью 5 настоящей статьи. Субъект персональных данных вправе требовать от оператора уточнения своих персональных данных, их блокирования или уничтожения в случае, если персональные данные являются не-

полными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

2. Сведения о наличии персональных данных должны быть предоставлены субъекту персональных данных оператором в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных.

3. Доступ к своим персональным данным предоставляется субъекту персональных данных или его законному представителю оператором при обращении либо при получении запроса субъекта персональных данных или его законного представителя. Запрос должен содержать номер основного документа, удостоверяющего личность субъекта персональных данных или его законного представителя, сведения о дате выдачи указанного документа и выдавшем его органе и собственноручную подпись субъекта персональных данных или его законного представителя. Запрос может быть направлен в электронной форме и подписан электронной цифровой подписью в соответствии с законодательством Российской Федерации.

4. Субъект персональных данных имеет право на получение при обращении или при получении запроса информации, касающейся обработки его персональных данных, в том числе содержащей:

1) подтверждение факта обработки персональных данных оператором, а также цель такой обработки;

2) способы обработки персональных данных, применяемые оператором;

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

4) перечень обрабатываемых персональных данных и источник их получения;

5) сроки обработки персональных данных, в том числе сроки их хранения;

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

5. Право субъекта персональных данных на доступ к своим персональным данным ограничивается в случае, если:

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

2) обработка персональных данных осуществляется органами, осуществившими задержание субъекта персональных данных по подозрению в совершении преступления, либо предъявившими субъекту персональных данных обвинение по уголовному делу, либо применившими к субъекту персональных данных меру пресечения до предъявления обвинения, за исключением предусмотренных уголовно-процессуальным законодательством Российской Федерации случаев, если допускается ознакомление подозреваемого или обвиняемого с такими персональными данными;

3) предоставление персональных данных нарушает конституционные права и свободы других лиц.

Статья 15. Права субъектов персональных данных при обработке их персональных данных в целях продвижения товаров, работ, услуг на рынке, а также в целях политической агитации.

1. Обработка персональных данных в целях продвижения товаров, работ, услуг на рынке путем осуществления прямых контактов с потенциальным потребителем с помощью средств связи, а также в целях политической агитации допускается только при условии предварительного согласия субъекта персональных данных. Указанная обработка персональных данных признается осуществляемой без предварительного согласия субъекта персональных данных, если оператор не докажет, что такое согласие было получено.

2. Оператор обязан немедленно прекратить по требованию субъекта персональных данных обработку его персональных данных, указанную в части 1 настоящей статьи.

Статья 16. Права субъектов персональных данных при принятии решений на основании исключительно автоматизированной обработки их персональных данных.

1. Запрещается принятие на основании исключительно автоматизированной обработки персональных данных решений, порождающих юридические последствия в отношении субъекта персональных данных или иным образом затрагивающих его права и законные интересы, за исключением случаев, предусмотренных частью 2 настоящей статьи.

2. Решение, порождающее юридические последствия в отношении субъекта персональных данных или иным образом затрагивающее его права и законные интересы, может быть принято на основании исключительно автоматизированной обработки его персональных данных только при наличии согласия в письменной форме субъекта персональных данных или в случаях, предусмотренных федеральными законами, устанавливающими также меры по обеспечению соблюдения прав и законных интересов субъекта персональных данных.

3. Оператор обязан разъяснить субъекту персональных данных порядок принятия решения на основании исключительно автоматизированной обработки его персональных данных и возможные юридические последствия такого решения, предоставить возможность заявить возражение против такого решения, а также разъяснить порядок защиты субъектом персональных данных своих прав и законных интересов.

4. Оператор обязан рассмотреть возражение, указанное в части 3 настоящей статьи, в течение семи рабочих дней со дня его получения и уведомить субъекта персональных данных о результатах рассмотрения такого возражения.

ПРИЛОЖЕНИЕ 2

Закон Российской Федерации "О государственной тайне" (от 21 июля 1993 г. № 5485-1) (извлечения)

Статья 5. Перечень сведений, составляющих государственную тайну.

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;

об объемах запасов, добычи, передачи и потребления платины, металлов платиновой группы, природных алмазов, а также об объемах других 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-розыскной деятельности:

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

о лицах, сотрудничающих или сотрудничавших на конфиденциальной основе с органами, осуществляющими разведывательную, контрразведывательную и оперативно-розыскную деятельность;

об организации, о силах, средствах и методах обеспечения безопасности объектов государственной охраны, а также данные о финансировании этой деятельности, если эти данные раскрывают перечисленные сведения;

о системе президентской, правительственной, шифрованной, в том числе кодированной и засекреченной связи, о шифрах, 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.

Статья 7. Сведения, не подлежащие отнесению к государственной тайне и засекречиванию.

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;

о состоянии экологии, здравоохранения, санитарии, демографии, образования, культуры, сельского хозяйства, а также о состоянии преступности;

о привилегиях, компенсациях и льготах, предоставляемых государством гражданам, должностным лицам, предприятиям, учреждениям и организациям;

о фактах нарушения прав и свобод человека и гражданина;

о размерах золотого запаса и государственных валютных резервах Российской Федерации;

о состоянии здоровья высших должностных лиц Российской Федерации;

о 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 суд.

ПРИЛОЖЕНИЕ 3

Федеральный Закон Российской Федерации
"О коммерческой тайне"
(от 29 июля 2004 г. № 98-ФЗ)
(извлечения)

Статья 3. Основные понятия, используемые в настоящем Федеральном законе.

Для целей настоящего Федерального закона используются следующие основные понятия:

1) коммерческая тайна - конфиденциальность информации, позволяющая ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду;

2) информация, составляющая коммерческую тайну, - научно-техническая, технологическая, производственная, финансово-экономическая или иная информация (в том числе составляющая секреты производства (ноу-хау)), которая имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к которой нет свободного доступа на законном основании и в отношении которой обладателем такой информации введен режим коммерческой тайны;

3) режим коммерческой тайны - правовые, организационные, технические и иные принимаемые обладателем информации, составляющей коммерческую тайну, меры по охране ее конфиденциальности;

4) обладатель информации, составляющей коммерческую тайну, - лицо, которое владеет информацией, составляющей коммерческую тайну, на законном основании, ограничило доступ к этой информации и установило в отношении ее режим коммерческой тайны;

5) доступ к информации, составляющей коммерческую тайну, - ознакомление определенных лиц с информацией, составляющей коммерческую тайну, с согласия ее обладателя или на ином законном основании при условии сохранения конфиденциальности этой информации;

6) передача информации, составляющей коммерческую тайну, - передача информации, составляющей коммерческую тайну и зафиксированной на материальном носителе, ее обладателем контрагенту на основании договора в объеме и на условиях, которые предусмотрены договором, включая условие о принятии контрагентом установленных договором мер по охране ее конфиденциальности;

7) контрагент - сторона гражданско-правового договора, которой обладатель информации, составляющей коммерческую тайну, передал эту информацию;

8) предоставление информации, составляющей коммерческую тайну, - передача информации, составляющей коммерческую тайну и зафиксированной на материальном носителе, ее обладателем органам государственной власти, иным государственным органам, органам местного самоуправления в целях выполнения их функций;

9) разглашение информации, составляющей коммерческую тайну, - действие или бездействие, в результате которых информация, составляющая ком-

мерческую тайну, в любой возможной форме (устной, письменной, иной форме, в том числе с использованием технических средств) становится известной третьим лицам без согласия обладателя такой информации либо вопреки трудовому или гражданско-правовому договору.

Статья 4. Право на отнесение информации к информации, составляющей коммерческую тайну, и способы получения такой информации.

1. 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.

2. Информация, самостоятельно полученная лицом при осуществлении исследований, систематических наблюдений или иной деятельности, считается полученной законным способом, несмотря на то, что содержание указанной информации может совпадать с содержанием информации, составляющей коммерческую тайну, обладателем которой является другое лицо.

3. Информация, составляющая коммерческую тайну, полученная от ее обладателя на основании договора или другом законном основании, считается полученной законным способом.

4. 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.

Статья 5. Сведения, которые не могут составлять 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 трав-

матизма и профессиональной заболеваемости, и о наличии свободных рабочих мест;

6) о задолженности работодателей по выплате заработной платы и по иным 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.

Статья 6. Предоставление информации, составляющей коммерческую тайну.

1. 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.

2. В случае отказа обладателя информации, составляющей коммерческую тайну, предоставить ее органу государственной власти, иному государственному органу, органу местного самоуправления данные органы вправе затребовать эту информацию в судебном порядке.

3. Обладатель информации, составляющей коммерческую тайну, а также органы государственной власти, иные государственные органы, органы местного самоуправления, получившие такую информацию в соответствии с частью 1 настоящей статьи, обязаны предоставить эту информацию по запросу судов, органов прокуратуры, органов предварительного следствия, органов дознания по делам, находящимся в их производстве, в порядке и на основаниях, которые предусмотрены законодательством Российской Федерации.

4. На документах, предоставляемых указанным в частях 1 и 3 настоящей статьи органам и содержащих информацию, составляющую коммерческую тайну, должен быть нанесен гриф "Коммерческая тайна" с указанием ее обладателя (для юридических лиц - полное наименование и место нахождения, для индивидуальных предпринимателей - фамилия, имя, отчество гражданина, являющегося индивидуальным предпринимателем, и место жительства).

Статья 7. Права обладателя информации, составляющей коммерческую тайну.

1. Права обладателя информации, составляющей коммерческую тайну, возникают с момента установления им в отношении такой информации режима

коммерческой тайны в соответствии со статьей 10 настоящего Федерального закона.

2. Обладатель информации, составляющей коммерческую тайну, имеет право:

1) устанавливать, изменять и 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) вводить в гражданский оборот информацию, составляющую коммерческую тайну, на основании договоров, предусматривающих включение в них условий об охране конфиденциальности этой информации;

5) требовать от юридических и физических лиц, получивших доступ к информации, составляющей коммерческую тайну, органов государственной власти, иных государственных органов, органов местного самоуправления, которым предоставлена информация, составляющая коммерческую тайну, соблюдения обязанностей по охране ее конфиденциальности;

6) требовать от лиц, получивших доступ к информации, составляющей коммерческую тайну, в результате действий, осуществленных случайно или по ошибке, охраны конфиденциальности этой информации;

7) 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.

Статья 8. Обладатель информации, составляющей коммерческую тайну, полученной в рамках трудовых отношений.

1. Обладателем информации, составляющей коммерческую тайну, полученной в рамках трудовых отношений, является работодатель.

2. В случае получения работником в связи с выполнением своих трудовых обязанностей или конкретного задания работодателя результата, способного к правовой охране в качестве изобретения, полезной модели, промышленного образца, топологии интегральной микросхемы, программы для электронных вычислительных машин или базы данных, отношения между работником и работодателем регулируются в соответствии с законодательством Российской Федерации об интеллектуальной собственности.

ПРИЛОЖЕНИЕ 4

Основные виды конфиденциальной информации принятые в законодательстве Российской Федерации

Виды информации с ограниченным доступом	***Правовая регламентация защиты***
I. Сведения, составляющие государственную тайну	
Государственная тайна.	Закон РФ "О государственной тайне". Закон РФ "Об информации, информационных технологиях и защите информации". Уголовный кодекс РФ.
II.Сведения конфиденциального характера	
Сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (персональные данные), за исключением сведений, подлежащих распространению в средствах массовой информации (СМИ) в установленных федеральными законами случаях.	Закон РФ "Об информации, информационных технологиях и защите информации". Закон РФ "О персональных данных". Уголовный кодекс РФ. Гражданский кодекс РФ. Семейный кодекс РФ. Трудовой кодекс РФ. Кодекс РФ об административных правонарушениях.
Сведения, составляющие тайну следствия и судопроизводства.	Уголовно-процессуальный Кодекс РФ. Уголовный кодекс РФ. Кодекс РФ об административных правонарушениях.
Служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом РФ и федеральными законами (служебная тайна).	Закон РФ "О государственной гражданской службе в РФ". Уголовный кодекс РФ. Гражданский кодекс РФ. Трудовой кодекс РФ. "Перечень сведений конфиденциального характера". "Положение о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти".
III.Сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией РФ и федеральными законами	
Банковская тайна.	Закон РСФСР "О банках и банковской деятельности". Уголовный кодекс РФ. Гражданский кодекс РФ.

Виды информации с ограниченным доступом	***Правовая регламентация защиты***
Тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений.	Закон РФ "О связи". Закон РФ "О почтовой связи". Закон РФ "О частной детективной и охранной деятельности в РФ". Уголовный Кодекс РФ.
Сведения о мерах безопасности, применяемых в отношении судей, участников уголовного процесса, должностных лиц правоохранительных и контролирующих органов, а также их близких.	Закон РФ "О государственной защите судей, должностных лиц правоохранительных и контролирующих органов". Уголовный Кодекс РФ.
Тайна государственной охранной деятельности.	Закон РФ "О государственной охране". Гражданский Кодекс РФ.
Тайна голосования.	Уголовный Кодекс РФ. Кодекс РФ об административных правонарушениях.
Нотариальная тайна.	Основы законодательства РФ о нотариате. Гражданский Кодекс РФ.
Тайна страхования.	Гражданский Кодекс РФ. Закон РФ "О страховании". Закон РФ "Об индивидуальном (персонифицированном) учете в системе государственного пенсионного страхования".
Врачебная тайна.	Основы законодательства РФ об охране здоровья граждан.
Музейная тайна (сведения о музейных предметах негосударственного фонда РФ).	Закон РФ "О музейном фонде РФ и музеях в РФ".
Геологическая и иная информация о недрах	Закон РФ "О недрах".
Редакционная и журналистская тайны.	Закон РФ "О средствах массовой информации".
Сведения, связанные с коммерческой деятельностью.	Закон РФ "О коммерческой тайне". Уголовный Кодекс РФ. Гражданский Кодекс РФ. Трудовой кодекс РФ.
Сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации информации о них.	Патентный Закон РФ. Уголовный Кодекс РФ. Гражданский кодекс РФ. Кодекс РФ об административных правонарушениях.

ПРИЛОЖЕНИЕ 5

«УТВЕРЖДАЮ»
Руководитель предприятия
_____
(наименование предприятия)
_____
(подпись, фамилия и инициалы)
«____» _____ 200___г.

ЭКСПЕРТНОЕ ЗАКЛЮЧЕНИЕ

Экспертная комиссия _____,
(наименование предприятия)
назначенная приказом руководителя _____
(наименование предприятия)
от «___» _____ 200___г. №____, рассмотрев материалы _____
_____,
(вид материалов, фамилия, имя, отчество автора, полное название работы)
подтверждает, что в материалах _____
(указать, содержатся или не содержатся сведения, запрещенные к открытому опубликованию).

В работе экспертной комиссии принимали участие: _____
_____
(перечисляются должностные лица с указанием должностей и наименований предприятий)

На публикацию материалов _____
(следует или нет) получить согласие в органе государственной власти, на предприятии.

Заключение: _____.
(отражается вывод о возможности или невозможности открытого опубликования материалов)

Председатель комиссии _____
(подпись, фамилия и инициалы)
Члены комиссии _____
(подпись, фамилия и инициалы)
_____
(подпись, фамилия и инициалы)

ПРИЛОЖЕНИЕ 6

Основные принципы общения с представителями СМИ

Разговаривать с прессой можно по-разному и по различным поводам. Общение с ее представителями может быть продиктовано необходимостью довести до массовой аудитории официальное сообщение, точку зрения руководства предприятия или соответствующий комментарий. В этом случае вы являетесь инициатором встречи, и рассчитывать следует только на положительный результат. Сложнее обстоит дело, когда пресса сама выходит на вас с просьбой прокомментировать ту или иную ситуацию. И если в первом случае ваши пожелания могут не совпасть, то здесь вы выступаете в роли стороны, "принуждаемой к ответу". Ваше незавидное положение заключается в том, что вы, хотите или не хотите, вынуждены откликнуться на просьбу о встрече, причем сделать это необходимо оперативно и грамотно в условиях сжатого времени, потому что, если на контакт не пойдете вы, то найдется масса комментаторов различного толка и с легкой руки "независимых экспертов" будет нарисована такая картина ситуации, что вам впоследствии предстоит долго и упорно разъяснять, что к чему.

Однако прежде чем "ринуться на амбразуру", необходимо запомнить или хотя бы постараться следовать некоторым принципам, которые надо иметь в виду при общении с прессой. Большая их часть носит запретительный характер, ограничивающий, казалось бы, вашу "свободу слова". Но эти запреты - только во благо.

Принцип 1. ***Никогда не говорите неправды***. Любая ложь рано или поздно будет раскрыта, и тогда потребуется много усилий, чтобы восстановить подорванное доверие не только по отношению к вам лично, но и в целом ко всему предприятию.

Принцип 2. ***Никогда ничего не выдумывайте***. Нельзя позволить себе поддаться давлению со стороны корреспондента, чтобы тот тут же радостно сообщил в редакцию: "Я выбил у него это признание!" Потом трудно будет объяснить, что, мол, "ничего такого" вы не говорили, он "сам все додумал". Если вы не знаете ответа на вопрос - так и скажите, добавив при этом, что не хотите показаться необъективным и постараетесь выяснить детали, а позже непременно поделитесь с прессой достоверной информацией.

Принцип 3. ***Никогда не комментируйте того, о чем у вас нет четкого представления,*** тем более, если направленность разговора выходит за рамки ваших прямых функциональных обязанностей. Не позволяйте втягивать себя в гипотетические дискуссии, особенно на политические темы (даже со ссылкой на свое личное мнение). Придерживайтесь рамок оговоренной ранее проблематики беседы.

Принцип 4. ***Никогда не давайте волю вашим чувствам***. Соглашаясь на интервью, помните: ваше лицо - это лицо предприятия. Ни в коем случае не позволяйте себе проявлений грубости, бестактности, раздражительности. Оставайтесь спокойным, рассудительным и, по возможности, обаятельным.

Принцип 5. ***Никогда не подвергайте критике дело, которому служите.*** Охотников до этого и так предостаточно. Сдержанная критика допустима, если она носит конструктивный характер и направлена на изменение ситуации к лучшему.

Принцип 6. ***Никогда не комментируйте слухи и мнения других людей***. Придерживайтесь только достоверных фактов.

Принцип 7. ***Никогда не раскрывайте информацию ограниченного распространения***. Перед встречей с представителями СМИ обязательно уточните у лиц, которые готовили материалы для встречи. Не берите на встречу с представителями СМИ документы, содержащие государственную, коммерческую или иную специально охраняемую законом тайну. Они имеют неприятную привычку выпадать из папки в самый неподходящий момент. Для облегчения своего общения с представителями СМИ оговорите заранее, что такие-то темы затрагиваться не будут. Примите меры к тому, чтобы по маршруту следования и в помещении, куда приглашены журналисты, схемы, карты, таблицы, которые содержат информацию ограниченного распространения, были зачехлены, а на мониторах информационных систем были специальные заставки. При необходимости можно заранее оговорить и ракурсы съемок. Помните, что проносимая видеокамера может случайно находится во включенном состоянии, а диктофон может быть непроизвольно включен журналистом еще до начала мероприятия.

Принцип 8. ***Никогда не нарушайте обещаний***. Работа редакционного цеха зависима от информации, и под ваше интервью может быть оставлено место. Сорванная встреча или не предоставленные к условленному сроку данные вернутся к вам бумерангом в гипертрофированном виде.

Принцип 9. ***Никогда не говорите: "Без комментариев"*** (пресловутое английское "No comments"). Всегда можно найти способ ответить на вопрос, даже если вы не знаете ответ или не можете говорить на какую-то определенную тему. Отказ отвечать журналисту создает впечатление, что ответ-то вы знаете, но не хотите "раскрывать страшную тайну".

Принцип 10. ***Никогда не думайте плохо о журналистах***. С таким настроем лучше к прессе не выходить!

Правила ведения телеинтервью делятся на два блока: поведенческий и содержательный. Причем они настолько взаимосвязаны и взаимозависимы, что недоработка одного из них ведет к провалу всего мероприятия.

Содержательный блок

Правило 1. ***Держите в уме заготовленные заранее тезисы***. При любом ответе на вопрос старайтесь развернуть его так, чтобы ваш ответ убедил зрителя, что вы откомментировали именно ту проблему, которая была перед вами поставлена.

Правило 2. ***Не спешите отвечать на вопрос, подумайте***. Даже если интервью идет в прямом эфире, несколько секунд на обдумывание ответа иной раз того стоят.

Правило 3. ***Старайтесь вести свою линию***. Если вы чувствуете, что интервью идет к своему завершению, а нужный вам тезис не прозвучал, следует выбрать удобный момент и задать самому вслух вопрос, на который у вас готов ответ.

Правило 4. ***Избегайте односложных ответов***. Вам предоставлена возможность довести свою точку зрения до зрителя, и ваша задача максимально ее использовать. Короткие фразы могут быть использованы лишь для усиления драматичности ситуации, демонстрации решимости исправить положение.

Правило 5. ***Не отвечайте вопросом на вопрос***. Зритель рассчитывает получить вашу точку зрения, а не дополнительную головоломку.

Правило 6. ***Избегайте излишней статистики***. Нагромождение цифр затрудняет восприятие основной мысли. Кроме того, статистика относительна, и вас всегда можно будет впоследствии обвинить в неточности и, что еще хуже, в неинформированности.

Правило 7. ***Используйте простой разговорный язык***, и вас не уличат в зазубривании текста ответов, подготовленных заранее и поэтому, как правило, имеющих характер формальных, четко нарезанных фраз.

Правило 8. ***Не следует казаться фамильярным***. Не обращайтесь к корреспонденту по имени. Может сложиться впечатление, что вы давно находитесь в приятельских отношениях, и он при любом раскладе на вашей стороне, что вызовет недоверие у зрителя к сказанному вами.

Правило 9. ***Используйте принцип акцентированной концовки***. Корреспондент заинтересован в завершении интервью "на высокой ноте". Помогите ему в этом, когда почувствуете, что ваша беседа близится к завершению.

Поведенческий блок

Здесь самое важное - постараться вести себя как можно более естественно.

Правило 1. ***Никогда не смотрите в камеру***. Лучше всего о ней вообще забыть. Вы разговариваете со своим собеседником, поэтому и смотреть надо на него. Если вы общаетесь с группой журналистов, обращайтесь к тому, кто задал вопрос.

Правило 2. ***Не опускайте глаза и не отводите взгляд в сторону***. Вас можно уличить в неискренности, но хуже того - в "даче заведомо ложных показаний".

Правило 3. ***Не поднимайте глаза к потолку, а тем более их не закатывайте***. Кроме эстетически неприглядного вида ваших белков сложится впечатление, что все это мероприятие вам порядком надоело. Да и ответа на поставленный вопрос вы на потолке не найдете.

Правило 4. ***Держитесь спокойно, с достоинством***. Не раскачивайтесь в кресле из стороны в сторону, взад-вперед. Мало того, что это совсем не свидетельствует о вашей мнимой расслабленности, это еще не повод говорить о вашем внутреннем волнении, а то и психическом дискомфорте. Да и стоящий перед вами микрофон не повторяет в такт ваши движения, а посему звук будет "плавать". Не держитесь за микрофон!

Правило 5. ***Следите за выражением вашего лица***. Оно должно гармонировать с содержанием сказанного. Понятно, что улыбка производит более благоприятное впечатление, чем печальный вид. Разговор о несчастье "с улыбкой на устах" может запомниться надолго.

Правило 6. ***Сохраняйте внутреннее спокойствие***. Даже если вам кажется, что вопрос поставлен некорректно, а то и вовсе провокационно, не теряйте самообладания. Ваше раздражение по отношению к корреспонденту вызовет ответный всплеск неприятия вашей персоны у зрителя, а при умелом монтаже и неприязнь.

Правило 7. ***Не складывайте руки на груди***. Это говорит о том, что вы не готовы к открытому диалогу, а то и вообще ушли в глухую защиту.

Правило 8. ***Не держите руки в карманах***. Это говорит о вашей неопрятности, неуважении к собеседнику и даже может свидетельствовать о недостоверности предоставляемых вами сведений. Кроме того, неизбежно возникнет со-

блазн поиграть мелочью и позвенеть ключами, а это - ненужное шумовое сопровождение.

Правило 9. ***Не ставьте руки на бедра***. Это - показатель вашего агрессивного настроения.

Правило 10. ***В положении сидя положите руки на стол***. Можно держать кулак одной руки в ладони другой, однако при этом не перебирайте большими пальцами, ибо эти движения отвлекают зрителя.

Правило 11. ***Не стучите по столу кулаком, пальцами или каким-либо предметом, оказавшимся в руках***. Если это авторучка, не щелкайте ею, а тем более не разбирайте ее на части.

Правило 12. ***Входе интервью стоя позвольте рукам принять естественное положение***, пусть даже они располагаются вдоль туловища. В этом случае ваш вид не будет таким уж неловким, как это вам самим может показаться.

Правило 13. ***Не размахивайте руками, подкрепляя жестами сказанное***. Оператор может не рассчитать длину ваших верхних конечностей, и они простонапросто "выпадут из кадра". Но уж если вы обычно помогаете себе жестикуляцией, держитесь в рамках приличия.

Правило 14. ***Не прикрывайте рукою рот***. Кроме нарушения артикуляции этот жест может рассматриваться как неуверенность и стыдливость.

Правило 15. ***Не сидите с расставленными широко ногами, положив руки на колени***. Такая позиция означает либо готовность к схватке, либо желание побыстрее покинуть место действия, что для вас не подходит.

Правило 16. ***Не сидите нога на ногу***. Не вы смотрите телевизор, а смотрят на вас. Мнимая расслабленность - не лучший для вас союзник. Кроме того, такая поза создает невидимый барьер между вами и корреспондентом. Вполне допустимо скрестить ноги в области лодыжек. При этом надо следить за тем, чтобы носки были темного цвета и покрывали икры.

Радиоинтервью имеет несколько особенностей, которые нельзя не учитывать.

Правило 1. ***Не пользуйтесь шпаргалками!*** Вы думаете, если вас не видно, то можно уткнуться в текст и индифферентным голосом его озвучивать. Не обольщайтесь! Шуршание листов бумаги и не замечаемая для вас скованность выдадут вас с потрохами.

Правило 2. ***Говорите законченными предложениями***. Это помогает редактору работать над плавностью звучания вашего голоса.

Правило 3. ***Не делайте частых и продолжительных пауз в прямом эфире***. Если на телеэкране картинка сглаживает этот недостаток, то "замолчавший" радиоприемник выглядит странно.

Правило 4. ***Не заполняйте паузы мычанием, кашлем и вздохами***. Это еще хуже, чем молчать!

Правило 5. ***Избегайте слов-паразитов***. Некоторые люди, так сказать, не подозревают, как, в общем, часто они их употребляют и так далее, пока не прослушают, в принципе, запись своего как бы интервью.

ПРИЛОЖЕНИЕ 7

_____
(согласен, не согласен)
Прокурор _____
(наименование органа прокуратуры,
_____
классный чин, фамилия, инициалы прокурора)
_____
(подпись)
"___" _____ г.

Постановление
о производстве обыска (выемки)

_____ "___" _____ г.
(место составления)

Следователь (дознаватель) _____
(наименование органа предварительного следствия или дознания,
_____,
классный чин или звание, фамилия, инициалы следователя (дознавателя)
рассмотрев материалы уголовного дела № _____, установил:
_____
(излагаются основания производства обыска (выемки)

На основании изложенного и руководствуясь частями первой и второй ст. 182 (частью первой или третьей ст. 183) УПК РФ, постановил:

1. Произвести обыск (выемку) _____
(где именно: указать, какие именно предметы,
_____
документы, ценности, имеющие значение для уголовного дела, подлежат изъятию)

2. Копию настоящего постановления направить прокурору _____
_____
(наименование органа прокуратуры)

Следователь (дознаватель) _____
(подпись)

Постановление мне предъявлено "___"_____ г. в ____ ч ____ мин
_____
(фамилия, имя, отчество лица, у которого производится обыск (выемка)
_____
(подпись лица, у которого производится обыск (выемка)

Следователь (дознаватель) _____
(подпись)

ПРИЛОЖЕНИЕ 8

Протокол
обыска (выемки)

_____ "___" _____ г.
(место составления)

Обыск (выемка) начат _____ в ___ ч ___ мин
Обыск (выемка) окончен _____ в ___ ч ___ мин

Следователь (дознаватель) _____
(наименование органа предварительного следствия или дознания,

_____
классный чин или звание, фамилия, инициалы следователя (дознавателя)

в присутствии понятых:

1. _____
(фамилия, имя, отчество и место жительства понятого)

2. _____
(фамилия, имя, отчество и место жительства понятого)

и с участием _____
(процессуальное положение, фамилии, инициалы участвующих лиц)

на основании постановления от "____" _____ г. и в соответствии с частями четвертой-шестнадцатой ст. 182 **(**частями второй, третьей и пятой ст. 183) УПК РФ произвел обыск (выемку) _____
(где именно)

в целях отыскания и изъятия _____
(каких именно, предметов документов, ценностей,

_____
имеющих значение для уголовного дела)

Перед началом обыска (выемки) участвующим лицам разъяснены их права, ответственность, а также порядок производства обыска (выемки).

Участвующие лица: _____
(подпись)

_____
(подпись)

Понятым, кроме того, до начала обыска (выемки) разъяснены их права, обязанности и ответственность, предусмотренные ст. 60 УПК РФ.

_____
(подпись понятого)

_____
(подпись понятого)

Участвующим лицам также объявлено о применении технических средств

_____
(каких именно, кем именно)

Перед началом обыска (выемки) следователем (дознавателем) было предъявлено постановление о производстве обыска (выемки) от "___"_____г., после чего _____
(кому именно)

было предложено выдать _____
(указать, какие именно предметы, документы, ценности,

_____
имеющие значение для уголовного дела)

Указанные предметы, документы и ценности _____
(выданы добровольно либо
_____
изъяты принудительно)
В ходе обыска (выемки) изъято: _____
(излагаются обстоятельства производства обыска (выемки),
_____
предусмотренные частями десятой, тринадцатой и четырнадцатой ст. 182
_____
УПК РФ, перечень и индивидуальные признаки изъятых предметов, их упаковка)
В ходе обыска (выемки) проводилась _____
(фотосъемка, видео-, аудиозапись)
Перед началом, в ходе либо по окончании обыска (выемки) от участвующих лиц
_____
(их процессуальное положение, фамилии, инициалы)
заявления _____. Содержание заявлений: _____
(поступили, не поступили)
_____
Понятые: _____
(подпись)
_____
(подпись)
Иные участвующие лица: _____
(подпись)
_____
(подпись)
Протокол прочитан _____
(лично или вслух следователем (дознавателем)
Замечания к протоколу _____
(содержание замечаний либо указание на их отсутствие)
Понятые: _____
(подпись)
_____
(подпись)
Иные участвующие лица: _____
(подпись)
_____
(подпись)
Следователь: _____
(подпись)
Копию протокола получил: _____
(фамилия, имя, отчество лица, в помещении которого
_____
произведен обыск (выемка), или представителя администрации организации)
"___"_____ г.
_____
(подпись лица, получившего протокол)

ПРИЛОЖЕНИЕ 9

Уголовный кодекс Российской Федерации (принят Федеральным законом РФ от 13 июня 1996 г. № 63-ФЗ) (извлечения)

Статья 183. Незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну.

1. Собирание сведений, составляющих коммерческую, налоговую или банковскую тайну, путем похищения документов, подкупа или угроз, а равно иным незаконным способом - наказывается штрафом в размере до восьмидесяти тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного до шести месяцев либо лишением свободы на срок до двух лет.

2. Незаконные разглашение или использование сведений, составляющих коммерческую, налоговую или банковскую тайну, без согласия их владельца лицом, которому она была доверена или стала известна по службе или работе, - наказываются штрафом в размере до ста двадцати тысяч рублей или в размере заработной платы или иного дохода осужденного за период до одного года с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет либо лишением свободы на срок до трех лет.

3. Те же деяния, причинившие крупный ущерб или совершенные из корыстной заинтересованности, - наказываются штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет либо лишением свободы на срок до пяти лет.

4. Деяния, предусмотренные частями второй или третьей настоящей статьи, повлекшие тяжкие последствия, - наказываются лишением свободы на срок до десяти лет.

Статья 272. Неправомерный доступ к компьютерной информации.

1. Неправомерный доступ к охраняемой законом компьютерной информации, то есть 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 от ста тысяч 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 - наказываются лишением свободы на срок 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 275. Государственная измена.

Государственная измена, то есть 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 либо без такового.

Примечание. Лицо, совершившее преступления, предусмотренные настоящей статьей, а также статьями 276 и 278 настоящего 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 соверше-

ны иностранным гражданином или лицом без гражданства, - наказываются 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.

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.

ПРИЛОЖЕНИЕ 10

Кодекс Российской Федерации об административных правонарушениях (принят Федеральным законом РФ от 30 декабря 2001 г. № 195-ФЗ) (извлечения)

Статья 5.39. Отказ в предоставлении гражданину информации.

Неправомерный отказ в предоставлении гражданину собранных в установленном порядке документов, материалов, непосредственно затрагивающих права и свободы гражданина, либо несвоевременное предоставление таких документов и материалов, непредоставление иной информации в случаях, предусмотренных законом, либо предоставление гражданину неполной или заведомо недостоверной информации - влечет наложение административного штрафа на должностных лиц в размере от пяти до десяти минимальных размеров оплаты труда.

Статья 13.11. Нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных).

Нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных) - влечет предупреждение или наложение административного штрафа на граждан в размере от трех до пяти минимальных размеров оплаты труда; на должностных лиц - от пяти до десяти минимальных размеров оплаты труда; на юридических лиц - от пятидесяти до ста минимальных размеров оплаты труда.

Статья 13.12. Нарушение правил защиты информации.

1. Нарушение условий, предусмотренных лицензией на осуществление деятельности в области защиты информации (за исключением информации, составляющей государственную тайну), - влечет наложение административного штрафа на граждан в размере от трех до пяти минимальных размеров оплаты труда; на должностных лиц - от пяти до десяти минимальных размеров оплаты труда; на юридических лиц - от пятидесяти до ста минимальных размеров оплаты труда.

2. Использование несертифицированных информационных систем, баз и банков данных, а также несертифицированных средств защиты информации, если они подлежат обязательной сертификации (за исключением средств защиты информации, составляющей государственную тайну), - влечет наложение административного штрафа на граждан в размере от пяти до десяти минимальных размеров оплаты труда с конфискацией несертифицированных средств защиты информации или без таковой; на должностных лиц - от десяти до двадцати минимальных размеров оплаты труда; на юридических лиц - от ста до двухсот минимальных размеров оплаты труда с конфискацией несертифицированных средств защиты информации или без таковой.

3. Нарушение условий, предусмотренных лицензией на проведение работ, связанных с использованием и защитой информации, составляющей государственную тайну, созданием средств, предназначенных для защиты информации, составляющей государственную тайну, осуществлением мероприятий и (или)

оказанием услуг по защите информации, составляющей государственную тайну, - влечет наложение административного штрафа на должностных лиц в размере от двадцати до тридцати минимальных размеров оплаты труда; на юридических лиц - от ста пятидесяти до двухсот минимальных размеров оплаты труда.

4. Использование несертифицированных средств, предназначенных для защиты информации, составляющей государственную тайну, - влечет наложение административного штрафа на должностных лиц в размере от тридцати до сорока минимальных размеров оплаты труда; 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.

5. Грубое нарушение условий, предусмотренных лицензией на осуществление деятельности в области защиты информации (за исключением информации, составляющей государственную тайну), - влечет наложение административного штрафа на лиц, осуществляющих предпринимательскую деятельность без образования юридического лица, в размере от десяти до пятнадцати минимальных размеров оплаты труда или административное приостановление деятельности на срок до девяноста суток; на должностных лиц - от десяти до пятнадцати минимальных размеров оплаты труда; на юридических лиц - от ста до ста пятидесяти минимальных размеров оплаты труда или административное приостановление деятельности на срок до девяноста суток.

Примечание. Понятие грубого нарушения устанавливается Правительством Российской Федерации в отношении конкретного лицензируемого вида деятельности.

Статья 13.13. Незаконная деятельность в области защиты информации.

1. Занятие видами деятельности в области защиты информации (за исключением информации, составляющей государственную тайну) без получения в установленном порядке специального разрешения (лицензии), если такое разрешение (такая лицензия) в соответствии с федеральным законом обязательно (обязательна), - влечет наложение административного штрафа на граждан в размере от пяти до десяти минимальных размеров оплаты труда с конфискацией средств защиты информации или без таковой; на должностных лиц - от двадцати до тридцати минимальных размеров оплаты труда с конфискацией средств защиты информации или без таковой; на юридических лиц - от ста до двухсот минимальных размеров оплаты труда с конфискацией средств защиты информации или без таковой.

2. 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 - 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.

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.

Статья 20.16. Незаконная частная детективная или охранная деятельность.

1. Осуществление частной детективной или охранной деятельности без специального разрешения (лицензии) - влечет наложение административного штрафа на граждан в размере от десяти до пятнадцати минимальных размеров оплаты труда; на юридических лиц - от двухсот до трехсот минимальных размеров оплаты труда.

2. Создание в организации службы безопасности без специального разрешения (лицензии) - влечет наложение административного штрафа на руководителя организации в размере от сорока до пятидесяти минимальных размеров оплаты труда.

3. Осуществление негосударственными образовательными учреждениями деятельности по подготовке или переподготовке кадров для осуществления частной детективной или охранной деятельности без специального разрешения (лицензии) - влечет наложение административного штрафа на руководителя учреждения в размере от двадцати до тридцати минимальных размеров оплаты труда.

4. Оказание частных детективных или охранных услуг, либо не предусмотренных законом, либо с нарушением установленных законом требований - влечет наложение административного штрафа на частных детективов (охранников) в размере от десяти до пятнадцати минимальных размеров оплаты труда; на руководителей частных детективных или охранных организаций - от двадцати до тридцати минимальных размеров оплаты труда.

Статья 20.17. Нарушение пропускного режима охраняемого объекта.

Самовольное проникновение на охраняемый в установленном порядке объект - влечет наложение административного штрафа в размере от трех до пяти минимальных размеров оплаты труда.

Статья 20.23. Нарушение правил производства, хранения, продажи и приобретения специальных технических средств, предназначенных для негласного получения информации.

1. Нарушение правил производства, хранения, продажи и приобретения специальных технических средств, предназначенных для негласного получения информации, при наличии специального разрешения (лицензии) - влечет наложение административного штрафа на должностных лиц в размере от сорока до пятидесяти минимальных размеров оплаты труда.

2. Нарушение правил разработки, ввоза в Российскую Федерацию и вывоза из Российской Федерации, а также порядка сертификации, регистрации и учета специальных технических средств, предназначенных для негласного получения информации, - влечет наложение административного штрафа на граждан в

размере от двадцати до двадцати пяти минимальных размеров оплаты труда с конфискацией специальных технических средств, предназначенных для негласного получения информации; на должностных лиц - от тридцати до пятидесяти минимальных размеров оплаты труда с конфискацией специальных технических средств, предназначенных для негласного получения информации.

Статья 20.24. Незаконное использование специальных технических средств, предназначенных для негласного получения информации, в частной детективной или охранной деятельности.

Использование в частной детективной или охранной деятельности специальных технических средств, предназначенных для негласного получения информации и не предусмотренных установленными перечнями, - влечет наложение административного штрафа на частных детективов (охранников) в размере до двадцати минимальных размеров оплаты труда с конфискацией незаконно используемых специальных технических средств; на руководителей частных детективных или охранных организаций (объединений, ассоциаций), служб безопасности в организациях - от десяти до двадцати минимальных размеров оплаты труда.

ПРИЛОЖЕНИЕ 11

Гражданский кодекс Российской Федерации (часть первая) (принят Федеральным законом РФ от 30 ноября 1994 г. № 51-ФЗ) (извлечения)

Статья 12. Способы защиты гражданских прав.

Защита гражданских прав осуществляется путем:

признания права; восстановления положения, существовавшего до нарушения права, и пресечения действий, нарушающих право или создающих угрозу его нарушения;

признания оспоримой сделки недействительной и применения последствий ее недействительности, применения последствий недействительности ничтожной сделки;

признания недействительным акта государственного органа или органа местного самоуправления; самозащиты права;

присуждения к исполнению обязанности в натуре;

возмещения убытков;

взыскания неустойки;

компенсации морального вреда;

прекращения или изменения правоотношения;

неприменения судом акта государственного органа или органа местного самоуправления, противоречащего закону;

иными способами, предусмотренными законом.

Статья 139. Служебная и коммерческая тайна.

1. Информация составляет служебную или коммерческую тайну в случае, когда информация имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к ней нет свободного доступа на законном основании и обладатель информации принимает меры к охране ее конфиденциальности. Сведения, которые не могут составлять служебную или коммерческую тайну, определяются законом и иными правовыми актами.

2. Информация, составляющая служебную или коммерческую тайну, защищается способами, предусмотренными настоящим Кодексом и другими законами.

Лица, незаконными методами получившие информацию, которая составляет служебную или коммерческую тайну, обязаны возместить причиненные убытки. Такая же обязанность возлагается на работников, разгласивших служебную или коммерческую тайну вопреки трудовому договору, в том числе контракту, и на контрагентов, сделавших это вопреки гражданско-правовому договору.

ПРИЛОЖЕНИЕ 12

Трудовой кодекс Российской Федерации (принят Федеральным законом РФ от 30 декабря 2001 г. № 197-ФЗ) (извлечения)

Статья 21. Основные права и обязанности работника.

Работник имеет право на:

заключение, изменение и расторжение трудового договора в порядке и на условиях, которые установлены настоящим Кодексом, иными федеральными законами;

предоставление ему работы, обусловленной трудовым договором;

рабочее место, соответствующее государственным нормативным требованиям охраны труда и условиям, предусмотренным коллективным договором;

своевременную и в полном объеме выплату заработной платы в соответствии со своей квалификацией, сложностью труда, количеством и качеством выполненной работы;

отдых, обеспечиваемый установлением нормальной продолжительности рабочего времени, сокращенного рабочего времени для отдельных профессий и категорий работников, предоставлением еженедельных выходных дней, нерабочих праздничных дней, оплачиваемых ежегодных отпусков;

полную достоверную информацию об условиях труда и требованиях охраны труда на рабочем месте;

профессиональную подготовку, переподготовку и повышение своей квалификации в порядке, установленном настоящим Кодексом, иными федеральными законами;

объединение, включая право на создание профессиональных союзов и вступление в них для защиты своих трудовых прав, свобод и законных интересов;

участие в управлении организацией в предусмотренных настоящим Кодексом, иными федеральными законами и коллективным договором формах;

ведение коллективных переговоров и заключение коллективных договоров и соглашений через своих представителей, а также на информацию о выполнении коллективного договора, соглашений;

защиту своих трудовых прав, свобод и законных интересов всеми не запрещенными законом способами;

разрешение индивидуальных и коллективных трудовых споров, включая право на забастовку, в порядке, установленном настоящим Кодексом, иными федеральными законами;

возмещение вреда, причиненного ему в связи с исполнением трудовых обязанностей, и компенсацию морального вреда в порядке, установленном настоящим Кодексом, иными федеральными законами;

обязательное социальное страхование в случаях, предусмотренных федеральными законами.

Работник обязан:

добросовестно исполнять свои трудовые обязанности, возложенные на него трудовым договором;

соблюдать правила внутреннего трудового распорядка;

соблюдать трудовую дисциплину;

выполнять установленные нормы труда;

соблюдать требования по охране труда и обеспечению безопасности труда;

бережно относиться к имуществу работодателя (в том числе к имуществу третьих лиц, находящемуся у работодателя, если работодатель несет ответственность за сохранность этого имущества) и других работников;

незамедлительно сообщить работодателю либо непосредственному руководителю о возникновении ситуации, представляющей угрозу жизни и здоровью людей, сохранности имущества работодателя (в том числе имущества третьих лиц, находящегося у работодателя, если работодатель несет ответственность за сохранность этого имущества).

Статья 81. Расторжение трудового договора по инициативе работодателя.

Трудовой договор может быть расторгнут работодателем в случаях:

6) однократного грубого нарушения работником трудовых обязанностей:

в) разглашения охраняемой законом тайны (государственной, коммерческой, служебной и иной), ставшей известной работнику в связи с исполнением им трудовых обязанностей;

11) представления работником работодателю подложных документов или заведомо ложных сведений при заключении трудового договора;

12) прекращения допуска к государственной тайне, если выполняемая работа требует допуска к государственной тайне;

14) в других случаях, установленных настоящим Кодексом и иными федеральными законами.

Статья 85. Понятие персональных данных работника. Обработка персональных данных работника.

Персональные данные работника - информация, необходимая работодателю в связи с трудовыми отношениями и касающаяся конкретного работника.

Обработка персональных данных работника - получение, хранение, комбинирование, передача или любое другое использование персональных данных работника.

Статья 86. Общие требования при обработке персональных данных работника и гарантии их защиты.

В целях обеспечения прав и свобод человека и гражданина работодатель и его представители при обработке персональных данных работника обязаны соблюдать следующие общие требования:

1) обработка персональных данных работника может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия работникам в трудоустройстве, обучении и продвижении по службе, обеспечения личной безопасности работников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества;

2) при определении объема и содержания обрабатываемых персональных данных работника работодатель должен руководствоваться Конституцией РФ, настоящим Кодексом и иными федеральными законами;

3) все персональные данные работника следует получать у него самого. Если персональные данные работника возможно получить только у третьей стороны, то работник должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие. Работодатель должен сообщить работнику о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа работника дать письменное согласие на их получение;

4) работодатель не имеет права получать и обрабатывать персональные данные работника о его политических, религиозных и иных убеждениях и частной жизни. В случаях, непосредственно связанных с вопросами трудовых отношений, в соответствии со статьей 24 Конституции РФ работодатель вправе получать и обрабатывать данные о частной жизни работника только с его письменного согласия;

5) работодатель не имеет права получать и обрабатывать персональные данные работника о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных федеральным законом;

6) при принятии решений, затрагивающих интересы работника, работодатель не имеет права основываться на персональных данных работника, полученных исключительно в результате их автоматизированной обработки или электронного получения;

7) защита персональных данных работника от неправомерного их использования или утраты должна быть обеспечена работодателем за счет его средств в порядке, установленном федеральным законом;

8) работники и их представители должны быть ознакомлены под расписку с документами организации, устанавливающими порядок обработки персональных данных работников, а также об их правах и обязанностях в этой области;

9) работники не должны отказываться от своих прав на сохранение и защиту тайны;

10) работодатели, работники и их представители должны совместно вырабатывать меры защиты персональных данных работников.

Статья 87. Хранение и использование персональных данных работников.

Порядок хранения и использования персональных данных работников в организации устанавливается работодателем с соблюдением требований настоящего Кодекса.

Статья 88. Передача персональных данных работника.

При передаче персональных данных работника работодатель должен соблюдать следующие требования:

не сообщать персональные данные работника третьей стороне без письменного согласия работника, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника, а также в случаях, установленных федеральным законом;

не сообщать персональные данные работника в коммерческих целях без его письменного согласия;

предупредить лиц, получающих персональные данные работника, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено.

Лица, получающие персональные данные работника, обязаны соблюдать режим секретности (конфиденциальности). Данное положение не распространяется на обмен персональными данными работников в порядке, установленном федеральными законами;

осуществлять передачу персональных данных работника в пределах одной организации в соответствии с локальным нормативным актом организации, с которым работник должен быть ознакомлен под расписку;

разрешать доступ к персональным данным работников только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные работника, которые необходимы для выполнения конкретных функций;

не запрашивать информацию о состоянии здоровья работника, за исключением тех сведений, которые относятся к вопросу о возможности выполнения работником трудовой функции;

передавать персональные данные работника представителям работников в порядке, установленном настоящим Кодексом, и ограничивать эту информацию только теми персональными данными работника, которые необходимы для выполнения указанными представителями их функций.

Статья 89. Права работников в целях обеспечения защиты персональных данных, хранящихся у работодателя.

В целях обеспечения защиты персональных данных, хранящихся у работодателя, работники имеют право на:

полную информацию об их персональных данных и обработке этих данных;

свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные работника, за исключением случаев, предусмотренных федеральным законом;

определение своих представителей для защиты своих персональных данных;

доступ к относящимся к ним медицинским данным с помощью медицинского специалиста по их выбору;

требование об исключении или исправлении неверных или неполных персональных данных, а также данных, обработанных с нарушением требований настоящего Кодекса. При отказе работодателя исключить или исправить персональные данные работника он имеет право заявить в письменной форме работодателю о своем несогласии с соответствующим обоснованием такого несогласия. Персональные данные оценочного характера работник имеет право дополнить заявлением, выражающим его собственную точку зрения;

требование об извещении работодателем всех лиц, которым ранее были сообщены неверные или неполные персональные данные работника, обо всех произведенных в них исключениях, исправлениях или дополнениях;

обжалование в суд любых неправомерных действий или бездействия работодателя при обработке и защите его персональных данных.

Статья 90. Ответственность за нарушение норм, регулирующих обработку и защиту персональных данных работника.

Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных работника, несут дисциплинарную, администра-

тивную, гражданско-правовую или уголовную ответственность в соответствии с федеральными законами.

Статья 192. Дисциплинарные взыскания.

За совершение дисциплинарного проступка, то есть неисполнение или ненадлежащее исполнение работником по его вине возложенных на него трудовых обязанностей, работодатель имеет право применить следующие дисциплинарные взыскания:

1) замечание;

2) выговор;

3) увольнение по соответствующим основаниям.

Федеральными законами, уставами и положениями о дисциплине для отдельных категорий работников могут быть предусмотрены также и другие дисциплинарные взыскания.

Не допускается применение дисциплинарных взысканий, не предусмотренных федеральными законами, уставами и положениями о дисциплине.

Статья 193. Порядок применения дисциплинарных взысканий.

До применения дисциплинарного взыскания работодатель должен затребовать от работника объяснение в письменной форме. В случае отказа работника дать указанное объяснение составляется соответствующий акт.

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, а по результатам ревизии, проверки финансово-хозяйственной деятельности или аудиторской проверки - позднее двух лет со дня его совершения. В указанные сроки 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 государственные инспекции труда или органы по рассмотрению индивидуальных трудовых споров.

Статья 194. Снятие дисциплинарного взыскания.

Если в течение года со дня применения дисциплинарного взыскания работник не будет подвергнут новому дисциплинарному взысканию, то он считается не имеющим дисциплинарного взыскания.

Работодатель до истечения года со дня применения дисциплинарного взыскания имеет право снять его с работника по собственной инициативе, просьбе самого работника, ходатайству его непосредственного руководителя или представительного органа работников.

Статья 232. Обязанность стороны трудового договора возместить ущерб, причиненный ею другой стороне этого договора.

Сторона трудового договора (работодатель или работник), причинившая ущерб другой стороне, возмещает этот ущерб в соответствии с настоящим Кодексом и иными федеральными законами.

Трудовым договором или заключаемыми в письменной форме соглашениями, прилагаемыми к нему, может конкретизироваться материальная ответственность сторон этого договора. При этом договорная ответственность работодателя перед работником не может быть ниже, а работника перед работодателем - выше, чем это предусмотрено настоящим Кодексом или иными федеральными законами.

Расторжение трудового договора после причинения ущерба не влечет за собой освобождения стороны этого договора от материальной ответственности, предусмотренной настоящим Кодексом или иными федеральными законами.

Статья 233. Условия наступления материальной ответственности стороны трудового договора.

Материальная ответственность стороны трудового договора наступает за ущерб, причиненный ею другой стороне этого договора в результате ее виновного противоправного поведения (действий или бездействия), если иное не предусмотрено настоящим Кодексом или иными федеральными законами.

Каждая из сторон трудового договора обязана доказать размер причиненного ей ущерба.

Статья 238. Материальная ответственность работника за ущерб, причиненный работодателю.

Работник обязан возместить работодателю причиненный ему прямой действительный ущерб. Неполученные доходы (упущенная выгода) взысканию с работника не подлежат.

Под прямым действительным ущербом понимается реальное уменьшение наличного имущества работодателя или ухудшение состояния указанного имущества (в том числе имущества третьих лиц, находящегося у работодателя, если работодатель несет ответственность за сохранность этого имущества), а также необходимость для работодателя произвести затраты либо излишние выплаты на приобретение или восстановление имущества.

Работник несет материальную ответственность как за прямой действительный ущерб, непосредственно причиненный им работодателю, так и за ущерб, возникший у работодателя в результате возмещения им ущерба иным лицам.

Статья 239. Обстоятельства, исключающие материальную ответственность работника.

Материальная ответственность работника исключается в случаях возникновения ущерба вследствие непреодолимой силы, нормального хозяйственного риска, крайней необходимости или необходимой обороны либо неисполнения работодателем обязанности по обеспечению надлежащих условий для хранения имущества, вверенного работнику.

Статья 240. Право работодателя на отказ от взыскания ущерба с работника.

Работодатель имеет право с учетом конкретных обстоятельств, при которых был причинен ущерб, полностью или частично отказаться от его взыскания с виновного работника.

Статья 241. Пределы материальной ответственности работника.

За причиненный ущерб работник несет материальную ответственность в пределах своего среднего месячного заработка, если иное не предусмотрено настоящим Кодексом или иными федеральными законами.

Статья 242. Полная материальная ответственность работника.

Полная материальная ответственность работника состоит в его обязанности возмещать причиненный ущерб в полном размере.

Материальная ответственность в полном размере причиненного ущерба может возлагаться на работника лишь в случаях, предусмотренных настоящим Кодексом или иными федеральными законами.

Работники в возрасте до восемнадцати лет несут полную материальную ответственность лишь за умышленное причинение ущерба, за ущерб, причиненный в состоянии алкогольного, наркотического или токсического опьянения, а также за ущерб, причиненный в результате совершения преступления или административного проступка.

Статья 243. Случаи полной материальной ответственности.

Материальная ответственность в полном размере причиненного ущерба возлагается на работника в следующих случаях:

1) когда в соответствии с настоящим Кодексом или иными федеральными законами на работника возложена материальная ответственность в полном размере за ущерб, причиненный работодателю при исполнении работником трудовых обязанностей;

3) умышленного причинения ущерба;

4) причинения ущерба в состоянии алкогольного, наркотического или токсического опьянения;

5) причинения ущерба в результате преступных действий работника, установленных приговором суда;

6) причинения ущерба в результате административного проступка, если таковой установлен соответствующим государственным органом;

7) разглашения сведений, составляющих охраняемую законом тайну (служебную, коммерческую или иную), в случаях, предусмотренных федеральными законами;

8) причинения ущерба не при исполнении работником трудовых обязанностей.

Статья 248. Порядок взыскания ущерба.

Взыскание с виновного работника суммы причиненного ущерба, не превышающей среднего месячного заработка, производится по распоряжению работодателя. Распоряжение может быть сделано не позднее одного месяца со дня окончательного установления работодателем размера причиненного работником ущерба.

Если месячный срок истек или работник не согласен добровольно возместить причиненный работодателю ущерб, а сумма причиненного ущерба, подле-

жащая взысканию с работника, превышает его средний месячный заработок, то взыскание осуществляется в судебном порядке.

При несоблюдении работодателем установленного порядка взыскания ущерба работник имеет право обжаловать действия работодателя в суд.

Работник, виновный в причинении ущерба работодателю, может добровольно возместить его полностью или частично. По соглашению сторон трудового договора допускается возмещение ущерба с рассрочкой платежа. В этом случае работник представляет работодателю письменное обязательство о возмещении ущерба с указанием конкретных сроков платежей. В случае увольнения работника, который дал письменное обязательство о добровольном возмещении ущерба, но отказался возместить указанный ущерб, непогашенная задолженность взыскивается в судебном порядке.

С согласия работодателя работник может передать ему для возмещения причиненного ущерба равноценное имущество или исправить поврежденное имущество.

Возмещение ущерба производится независимо от привлечения работника к дисциплинарной, административной или уголовной ответственности за действия или бездействие, которыми причинен ущерб работодателю.

НОРМАТИВНО-ПРАВОВЫЕ АКТЫ И ЛИТЕРАТУРА, РЕКОМЕНДУЕМАЯ ДЛЯ САМОСТОЯТЕЛЬНОГО ИЗУЧЕНИЯ

1. Конституция Российской Федерации (принята на всенародном голосовании 12 декабря 1993 г., с изм., внесенными Указами Президента РФ от 9 января 1996 г. № 20, от 10 февраля 1996 г. № 173, от 9 июня 2001 г. № 679, от 25 июля 2003 г. № 841), справочная правовая система "Гарант".
2. Закон Российской Федерации от 21 июля 1993 г. № 5485-I "О государственной тайне" (с изм. и доп. от 6 октября 1997 г., 30 июня, 11 ноября 2003 г., 29 июня, 22 августа 2004 г.), справочная правовая система "Гарант".
3. Закон Российской Федерации от 27 декабря 1991 г. № 2124-I "О средствах массовой информации" (с изм. и доп. от 13 января, 6 июня, 19 июля, 27 декабря 1995 г., 2 марта 1998 г., 20 июня, 5 августа 2000 г., 4 августа 2001 г., 21 марта, 25 июля 2002 г., 4 июля, 8 декабря 2003 г., 29 июня, 22 августа, 2 ноября 2004 г., 21 июля 2005 г.), справочная правовая система "Гарант".
4. Закон Российской Федерации от 11 марта 1992 г. № 2487-I "О частной детективной и охранной деятельности в Российской Федерации" (с изм. и доп. от 21 марта 2002 г., 10 января 2003 г., 6 июня 2005 г.), справочная правовая система "Гарант".
5. Закон Российской Федерации от 10 июля 1992 г. № 3266-1 "Об образовании" (с изм. и доп. от 24 декабря 1993 г., 13 января 1996 г., 16 ноября 1997 г., 20 июля, 7 августа, 27 декабря 2000 г., 30 декабря 2001 г., 13 февраля, 21 марта, 25 июня, 25 июля, 24 декабря 2002 г., 10 января, 7 июля, 8 декабря, 23 декабря 2003 г., 5 марта, 30 июня, 20 июля, 22 августа, 29 декабря 2004 г., 9 мая, 18 июля, 21 июля 2005 г.), справочная правовая система "Гарант".
6. Закон Российской Федерации от 9 июля 1993 г. № 5351-I "Об авторском праве и смежных правах" (с изменениями от 19 июля 1995 г., 20 июля 2004 г.), справочная правовая система "Гарант".
7. Федеральный закон Российской Федерации от 13 января 1995 г. № 7-ФЗ "О порядке освещения деятельности органов государственной власти в государственных средствах массовой информации", справочная правовая система "Гарант".
8. Федеральный закон Российской Федерации от 15 июля 1995 г. № 101-ФЗ "О международных договорах Российской Федерации", справочная правовая система "Гарант".
9. Федеральный закон Российской Федерации от 3 апреля 1995 г. № 40-ФЗ "О федеральной службе безопасности" (с изм. и доп. от 30 декабря 1999 г., 7 ноября 2000 г., 30 декабря 2001 г., 7 мая, 25 июля 2002 г., 10 января, 30 июня 2003 г., 22 августа 2004 г., 7 марта 2005 г., 15 апреля, 27 июля 2006 г.), справочная правовая система "Гарант".
10. Федеральный закон Российской Федерации от 12 августа 1995 г. № 144-ФЗ "Об оперативно-розыскной деятельности" (с изм. и доп. от 18 июля 1997 г., 21 июля 1998 г., 5 января, 30 декабря 1999 г., 20 марта 2001 г., 10 января, 30 июня 2003 г., 29 июня, 22 августа 2004 г., 2 декабря 2005 г.), справочная правовая система "Гарант".
11. Федеральный закон Российской Федерации от 15 августа 1996 г. № 114-ФЗ "О порядке выезда из Российской Федерации и въезда в Российскую Федера-

цию" (с изм. и доп. от 18 июля 1998 г., 24 июня 1999 г., 10 января, 30 июня 2003 г., 29 июня 2004 г.), справочная правовая система "Гарант".
12. Федеральный закон Российской Федерации от 14 апреля 1999 г. № 77-ФЗ "О ведомственной охране", справочная правовая система "Гарант".
13. Федеральный закон Российской Федерации от 8 августа 2001 г. № 128-ФЗ "О лицензировании отдельных видов деятельности" (с изм. и доп. от 13, 21 марта, 9 декабря 2002 г., 10 января, 27 февраля, 11 марта, 26 марта, 23 декабря 2003 г., 2 ноября 2004 г., 21 марта, 2 июля 2005 г.), справочная правовая система "Гарант".
14. Федеральный закон Российской Федерации от 27 июля 2004 г. № 79-ФЗ "О государственной гражданской службе Российской Федерации" (с изм. и доп. от 2 февраля 2006 г.), справочная правовая система "Гарант".
15. Федеральный закон Российской Федерации от 29 июля 2004 г. № 98-ФЗ "О коммерческой тайне", справочная правовая система "Гарант".
16. Федеральный закон Российской Федерации от 13 марта 2006 г. № 38-ФЗ "О рекламе", справочная правовая система "Гарант".
17. Федеральный закон Российской Федерации от 27 июля 2006 г. № 149-ФЗ "О персональных данных", справочная правовая система "Гарант".
18. Федеральный закон Российской Федерации от 27 июля 2006 г. № 152-ФЗ "Об информации, информационных технологиях и о защите информации", справочная правовая система "Гарант".
19. Гражданский кодекс Российской Федерации часть первая от 30 ноября 1994 г. № 51-ФЗ, часть вторая от 26 января 1996 г. № 14-ФЗ и часть третья от 26 ноября 2001 г. № 146-ФЗ (с изменениями от 26 января, 20 февраля, 12 августа 1996 г., 24 октября 1997 г., 8 июля, 17 декабря 1999 г., 16 апреля, 15 мая, 26 ноября 2001 г., 21 марта, 14 ноября, 26 ноября 2002 г., 10 января, 26 марта, 11 ноября, 23 декабря 2003 г., 29 июня, 29 июля, 2 декабря, 29 декабря, 30 декабря 2004 г., 21 марта, 9 мая, 2 июля, 18 июля, 21 июля 2005 г.), справочная правовая система "Гарант".
20. Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ (с изм. и доп. от 27 мая, 25 июня 1998 г., 9 февраля, 15 марта, 18 марта, 9 июля 1999 г., 9 марта, 20 марта, 19 июня, 7 августа, 17 ноября, 29 декабря 2001 г., 4 марта, 14 марта, 7 мая, 25 июня, 24 июля, 25 июля, 31 октября 2002 г., 11 марта, 8 апреля, 4 июля, 7 июля, 8 декабря 2003 г., 21 июля, 26 июля, 28 декабря 2004 г., 21 июля 2005 г., 1 октября 2006 г.), справочная правовая система "Гарант".
21. Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ (с изм. от 29 мая, 24 июля, 25 июля, 31 октября 2002 г., 30 июня, 4 июля, 7 июля, 8 декабря 2003 г., 22 апреля, 29 июня, 2 декабря, 28 декабря 2004 г., 1 июня 2005 г., 9 января, 3 марта, 3 июня, 3 июля, 27 июля 2006 г.), справочная правовая система "Гарант".
22. Кодекс Российской Федерации об административных правонарушениях от 30 декабря 2001 г. № 195-ФЗ (с изм. от 25 апреля, 25 июля, 30 октября, 31 октября, 31 декабря 2002 г., 30 июня, 4 июля, 11 ноября, 8 декабря, 23 декабря 2003 г., 9 мая, 26 июля, 28 июля, 20 августа, 25 октября, 28 декабря, 30 декабря 2004 г., 7 марта, 21 марта, 22 апреля, 9 мая, 2 июля, 21 июля, 22 июля, 27 сентября, 5 декабря, 19 декабря, 26 декабря, 27 декабря, 31 декабря 2005 г., 5 января, 2 февраля, 3 марта,16 марта, 15 апреля, 29 апреля, 8 мая, 3 июня, 3

июля, 18 июля, 26 июля, 27 июля, 16 октября, 5 ноября 2006 г.), справочная правовая система "Гарант".
23. Трудовой кодекс Российской Федерации от 30 декабря 2001 г. № 197-ФЗ (с изм. и доп. от 24 июля, 25 июля 2002 г., 30 июня 2003 г., 27 апреля, 22 августа, 29 декабря 2004 г., 9 мая 2005 г., 30 июня 2006 г.), справочная правовая система "Гарант".
24. Арбитражный процессуальный кодекс Российской Федерации от 24 июля 2002 г. № 95-ФЗ (с изм. и доп. от 28 июля, 2 ноября 2004 г., 31 марта, 27 декабря 2005 г.), справочная правовая система "Гарант".
25. Гражданский процессуальный кодекс Российской Федерации от 14 ноября 2002 г. № 138-ФЗ (с изм. и доп. от 30 июня 2003 г., 7 июня, 28 июля, 2 ноября, 29 декабря 2004 г., 21 июля, 27 декабря 2005 г.), справочная правовая система "Гарант".
26. Указ Президента Российской Федерации от 8 ноября 1995 г. № 1108 "О Межведомственной комиссии по защите государственной тайны" (с изм. от 6 октября 2004 г.), справочная правовая система "Гарант".
27. Указ Президента Российской Федерации от 30 ноября 1995 г. № 1203 "Об утверждении Перечня сведений, отнесенных к государственной тайне" (с изм. и доп. от 11 февраля 2006 г.), справочная правовая система "Гарант".
28. Указ Президента Российской Федерации от 6 марта 1997 г. № 188 "Об утверждении Перечня сведений конфиденциального характера", справочная правовая система "Гарант".
29. Указ Президента Российской Федерации от 17 декабря 1997 г. № 1300 "Об утверждении Концепции национальной безопасности Российской Федерации", справочная правовая система "Гарант".
30. Указ Президента Российской Федерации от 1 декабря 2000 г. № 1953 "Вопросы военно-технического сотрудничества Российской Федерации с иностранными государствами", справочная правовая система "Гарант".
31. Указ Президента Российской Федерации от 11 августа 2003 г. № 960 "Вопросы Федеральной службы безопасности Российской Федерации" (с изм. и доп. от 11 июля 2004 г., 31 августа, 1 декабря 2005 г., 12 июня, 27 июля 2006 г.), справочная правовая система "Гарант".
32. Указ Президента Российской Федерации от 6 октября 2004 г. № 1286 "Вопросы Межведомственной комиссии по защите государственной тайны", справочная правовая система "Гарант".
33. Доктрина информационной безопасности Российской Федерации, утверждена Президентом РФ от 9 сентября 2000 г. № Пр-1895, справочная правовая система "Гарант".
34. Распоряжение Президента Российской Федерации от 16 апреля 2005 г. № 151-рп "О перечне должностных лиц органов государственной власти, наделяемых полномочиями по отнесению сведений к государственной тайне", справочная правовая система "Гарант".
35. Постановление Правительства Российской Федерации от 5 декабря 1991 года № 35 "О перечне сведений, которые не могут составлять коммерческую тайну" (в ред. от 3 октября 2002 г.), справочная правовая система "Гарант".
36. Постановление Правительства Российской Федерации от 14 августа 1992 г. № 589 "Об утверждении Положения о вневедомственной охране при органах

внутренних дел Российской Федерации", справочная правовая система "Гарант".
37. Постановление Правительства Российской Федерации от 3 ноября 1994 г. № 1233 "Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти", справочная правовая система "Гарант".
38. Постановление Правительства Российской Федерации от 20 февраля 1995 г. № 170 "Об установлении порядка рассекречивания и продления сроков засекречивания архивных документов Правительства СССР", справочная правовая система "Гарант".
39. Постановление Правительства Российской Федерации от 15 апреля 1995 г. № 333 "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" (с изм. и доп. от 23 апреля 1996 г., 30 апреля 1997 г., 29 июля 1998 г., 3 октября 2002 г., 17 декабря 2004 г.), справочная правовая система "Гарант".
40. Постановление Правительства Российской Федерации от 26 июня 1995 г. № 608 "О сертификации средств защиты информации" (с изм. и доп. от 23 апреля 1996 г., 29 марта 1999 г., 17 декабря 2004 г.), справочная правовая система "Гарант".
41. Постановление Правительства Российской Федерации от 4 сентября 1995 г. № 870 "Об утверждении Правил отнесения сведений, составляющих государственную тайну, к различным степеням секретности", справочная правовая система "Гарант".
42. Постановление Правительства Российской Федерации от 28 октября 1995 г. № 1050 "Об утверждении Инструкции о порядке допуска должностных лиц и граждан Российской Федерации к государственной тайне" (с изм. и доп. от 8 августа 2003 г., 15 ноября 2004 г.), справочная правовая система "Гарант".
43. Постановление Правительства Российской Федерации от 2 августа 1997 г. № 973 "Об утверждении Положения о подготовке к передаче сведений, составляющих государственную тайну, другим государствам", справочная правовая система "Гарант".
44. Постановление Правительства Российской Федерации от 19 октября 1997 г. № 1598 "О порядке оформления разрешений на выезд из Российской Федерации военнослужащих Вооруженных Сил Российской Федерации, а также федеральных органов исполнительной власти, в которых предусмотрена военная служба", справочная правовая система "Гарант".
45. Постановление Правительства Российской Федерации от 22 августа 1998 г. № 1003 "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", справочная правовая система "Гарант".
46. Постановление Правительства Российской Федерации от 18 октября 2000 г. № 796 "Об утверждении Положения о лицензировании образовательной деятельности" (с изм. и доп. от 3 октября 2002 г.), справочная правовая система "Гарант".

47. Постановление Правительства Российской Федерации от 1 октября 2001 г. № 701 "Об утверждении Программы обеспечения защиты государственной тайны в Российской Федерации на период до 2005 года", справочная правовая система "Гарант".
48. Постановление Правительства Российской Федерации от 1 ноября 2001 г. № 759 "Об утверждении Правил распространения периодических печатных изданий по подписке", справочная правовая система "Гарант".
49. Постановление Правительства Российской Федерации от 27 мая 2002 г. № 348 "Об утверждении Положения о лицензировании деятельности по разработке и (или) производству средств защиты конфиденциальной информации" (с изм. и доп. от 3 октября 2002 г., 17 декабря 2004 г.), справочная правовая система "Гарант".
50. Постановление Правительства Российской Федерации от 26 января 2006 г. № 45 "Об организации лицензирования отдельных видов деятельности", справочная правовая система "Гарант".
51. Постановление Правительства Российской Федерации от 18 сентября 2006 г. № 573 "О предоставлении социальных гарантий гражданам, допущенным к государственной тайне на постоянной основе, и сотрудникам структурных подразделений по защите государственной тайны", справочная правовая система "Гарант".
52. "Инструкция о порядке проведения специальных экспертиз по допуску предприятий, учреждений и организаций к проведению работ, связанных с использованием сведений, составляющих государственную тайну", утвержденная директором Федеральной службы безопасности Российской Федерации от 23 августа 1995 г. № 28.
53. Решение Межведомственной комиссии по защите государственной тайны от 13 марта 1996 г. № 3 "О документах по организации и проведению государственной аттестации руководителей предприятий, учреждений и организаций, ответственных за защиту сведений, составляющих государственную тайну".
54. Приказ Министерства здравоохранения Российской Федерации от 16 марта 1999 г. № 83 "О перечне медицинских противопоказаний для осуществления работы с использованием сведений, составляющих государственную тайну", справочная правовая система "Гарант".
55. "Перечень учебных заведений, осуществляющих подготовку специалистов по защите информации, свидетельство об окончании которых дает руководителям предприятий, учреждений и организаций право на освобождение от государственной аттестации", утвержден решением Межведомственной комиссии по защите государственной тайны Российской Федерации от 21 октября 1998 г. № 41.
56. "Государственная тайна в Российской Федерации", издание 2-е, дополненное, издательство Санкт-Петербургского университета, СПБ., 1997.
57. Безопасность России. Правовые, социально-экономические и научно-технические аспекты. Информационная безопасность. - М.: МГФ "Знание", ГЭИТИ, 2005.
58. Герасименко В., Малюк А. Основы защиты информации, М., 1997.
59. Демушкин А.С. Документы и тайна. - М., ООО "Городец-издат", 2003.

60. Жигулин Г.П., Новосадов С.Г., Яковлев А.Д. "Информационная безопасность", СПБ., 2003.
61. Закон Российской Федерации от 21 июля 1993 г. № 5485-1 "О государственной тайне" (с постатейным комментарием), СПБ., 1997.
62. Коровяковский Д.Г., Защита коммерческой тайны предприятия: теоретические и практические аспекты, научно-практический и теоретический журнал "Национальные интересы. Приоритеты и безопасность", 2005, № 3.
63. Лопатин В. Концепция развития законодательства в сфере информационной безопасности Российской Федерации, - М., 1998.
64. Михайлов В., Право на тайну, журнал "Закон", 1998, № 2.
65. Новик В.К. Христиан Гольдбах и Франц Эпинус (из истории шифровальных служб России XVIII века). Доклад на конференции "Математика и безопасность информационных технологий" (МаБИТ-03, МГУ, 23-24.10.2003г.)).
66. Организация и современные методы защиты информации: Методическое пособие/Под общей редакцией С.А.Диева, А.Г.Шаваева. - М.: Концерн "Банковский Деловой Центр", 1998.
67. Развитие правового обеспечения информационной безопасности (монография)/(А.А.Стрельцов и др.); под редакцией А.А.Стрельцова; Фонд Гражданских инициатив в Политике Интернет. - М.: Престиж, 2005.
68. Роуан Р. Очерки секретной службы. Из истории разведки, СПб, 1992.
69. Сборник "Нормативные правовые акты по защите государственной тайны", части 1 и 2, - М., 1998.
70. Сборник методических материалов в области защиты государственной тайны, Издательство РГГУ, - М., 1998.
71. Северин В.А. Коммерческая тайна в России. - М.: ЗЕРЦАЛО-М, 2007.
72. Стрельцов А.А. Обеспечение информационной безопасности России. Теоретические и методологические основы. Под. ред. В.А. Садовничего и В.П. Шерстюка. - М., 2004.
73. Стрельцов А.А. Цель, структура и методы правового обеспечения информационной безопасности Российской Федерации. Научные и методологические проблемы информационной безопасности: Сборник статей. Под. ред. В.П. Шерстюка. - М., 2004.
74. Уфимцев Ю.С. "Информационная безопасность государства и его силовых структур", - М., 4-й филиал Воениздата, 2000.
75. Чертопруд С.В. Законодательные акты по защите гостайны в Российской империи в начале XX века, журнал "Вопросы защиты информации", - М., № 4 (35), 1996).
76. Шерстюк В.П. МГУ: научные исследования в области информационной безопасности. Информационное общество, 2005, № 1.
77. Ярочкин В.И. Информационная безопасность. Учебник для студентов ВУЗов - М.: Академический Проект, 2005.

В 2009 году, Университет стал победителем многоэтапного конкурса в результате которого определены двенадцать ведущих Университетов России, которым присвоена категория «Национальный исследовательский университет». Министерством образования и науки Российской Федерации была утверждена программ его развития на 2009-2018 годы. В 2011 году Университет получил наименование «Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики».

КАФЕДРА МОНИТОРИНГА И ПРОГНОЗИРОВАНИЯ ИНФОРМАЦИОННЫХ УГРОЗ

Кафедра организована в 2002 году. Первоначальное название кафедры «Мониторинга и прогнозирования чрезвычайных ситуаций».
Кафедра готовила специалистов по направлениям подготовки «прикладная математика» и «организации и технологии защиты информации».
С 2011 года кафедра перешла на двухуровневую систему образования, началась подготовка бакалавров и магистров по направлению «информационная безопасность».

Жигулин Георгий Петрович

Организационное и правовое обеспечение информационной безопасности

Учебное пособие

В авторской редакции
Компьютерный набор и верстка Горбачёв Д.В.

Редакционно-издательский отдел Санкт–Петербургского государственного университета информационных технологий, механики и оптики

Лицензия ИД №00408 от 05.11.99.

Заведующая РИО Н.Ф. Гусарова

Тираж 100 экз. Подписано к печати
Заказ № 1325 Отпечатано на ризографе.