Министерство образования и науки Российской Федерации
Южно-Уральский государственный университет
Кафедра «Экономическая безопасность»

У9(2).я7
М692

Л.М. Михалина

КОНКУРЕНТНАЯ РАЗВЕДКА

Учебное пособие

Челябинск
Издательский центр ЮУрГУ
2017

ББК У9(2)-983.я7
УДК 005.332.4(075.8)
М692

Одобрено
учебно-методической комиссией
Высшей школы экономики и управления

Рецензент:
Согрина Н.С., Рябчук П.Г.

Михалина Л.М.

М692 **Конкурентная разведка: у**чебное пособие / Л.М. Михалина под ред. А.В. Карпушкиной. – Челябинск: Издательский центр ЮУрГУ, 2017. – 140 с.

Пособие содержит конспективное изложение теоретического материала дисциплины «Конкурентная разведка».

Пособие предназначено для студентов высшей школы экономики и управления ЮУрГУ, обучающихся по специальности 38.05.01 «Экономическая безопасность».

ББК У9(2)-983.я7
УДК 005.332.4(075.8)

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Учебное пособие «Конкурентная разведка» используется при изучении соответствующей дисциплины в программе подготовки студентов, обучающихся по специальности 38.05.01 «Экономическая безопасность».

Конкурентная разведка – одно из направлений работы специалистов, обеспечивающих экономическую безопасность предприятия (организации) путём постоянного сбора, анализа и актуализации информации, позволяющей определить конкурентные преимущества и конкурентные недостатки хозяйствующих субъектов: партнёров, контрагентов, конкурентов.

Поэтому в программе подготовке специалистов в области экономической безопасности предприятия (организации) этой дисциплине уделяется достойное внимание.

В результате изучения дисциплины студенты должны получить развернутое представление как о самой службе конкурентной разведки предприятия (организации), так и о направлениях и методах работы соответствующих специалистов, изучить правовую основу деятельности разведывательных подразделений компаний, цели и задачи их работы.

Пособие содержит конспективное изложение теоретического материала дисциплины «Конкурентная разведка» и может рассматриваться как **опорный конспект лекций.**

1. ОСНОВЫ ДЕЯТЕЛЬНОСТИ КОНКУРЕНТНОЙ РАЗВЕДКИ

1.1. Общая характеристика конкурентной разведки, её цели и задачи

Российское Общество профессионалов конкурентной разведки формулирует понятие «Конкурентная разведка» так: это новая стратегическая инициатива в бизнесе, нацеленная на все в мире бизнеса, что значимо для способности компании конкурировать, в ходе проведения которой **подлежат изучению**:

– прямые, косвенные, потенциальные конкуренты хозяйствующего субъекта (предприятия, организации, фирмы, бизнеса);

– клиенты хозяйствующего субъекта;

– господствующие (перспективные) технологии выпуска продукции (оказания услуг) в соответствующих отраслях экономики;

– продукция (товары и услуги), выпускаемые хозяйствующими субъектами, работающими в соответствующих отраслях экономики;

– деловая среда на соответствующих товарных и территориальных (местных, региональных, национальных, международных) рынках.

Конкурентную разведку можно рассматривать как специальный маркетинговый инструмент изучения конкурентной среды: целенаправленную, постоянную систему сбора, обработки, анализа конкурентных сведений и использования полученной объективной информации о деловой среде, ресурсах, бизнес - слабостях, планах конкурентов. Корпоративная служба конкурентной разведки функционирует исключительно в рамках существующего национального (международного) законодательства и этических норм. Её деятельность направлена на минимизацию возможных рисков для хозяйствующего субъекта в ходе его производственно-сбытовой деятельности, на получение им конкурентных преимуществ на товарных рынках и, в конечном счете, – дополнительной прибыли.

Сфера интересов корпоративной службы конкурентной разведки – тайная, но законная деятельность предприятия (организации) по сбору, анализу, хранению и использованию конфиденциальной информации, применение которой приносит хозяйствующему субъекту экономические выгоды.

Таким образом, можно утверждать, что конкурентная разведка – это специализированные подразделения предприятий (организаций), работающие с целью создания достаточной информационной базы для учета специфики целевых рынков при разработке соответствующих стратегических планов хозяйствующих субъектов.

Сфера интересов конкурентной разведки включает в себя не только существующие компании, реализующие товары или услуги, аналогичные тем, что производит хозяйствующий субъект, но и возможных в будущем конкурентов, а также – его поставщиков и потребителей (клиентов). Это обуслов-

лено тем, что современная концепция конкуренции представляет собой схему внешних факторов воздействия, несущих в себе как перспективы, так и угрозы для бизнеса.

Следовательно, с учетом специфики соответствующей службы (соответствующего подразделения) предприятия, **конкурентная разведка** – это:

- с одной стороны – проводимые в рамках закона и с соблюдением этических норм сбор и обработка данных из разных источников, осуществляемый для выработки управленческих решений с целью повышения конкурентоспособности коммерческого предприятия (организации), а с другой стороны – структурное подразделение предприятия (организации), выполняющее вышеназванные функции;
- законный инструмент менеджмента товаропроизводителя, оказывающий помощь руководителям и менеджерам предприятия (организации) в принятии стратегических решений в рамках производственно – сбытовой деятельности соответствующего хозяйствующего субъекта;
- часть стратегического менеджмента предприятия (организации), направленная на поиск, добывание, обработку данных, создание информационных отчетов о рисках, угрозах, возможностях внешней среды хозяйствующего субъекта для обеспечения объективных условий принятия наиболее рациональных управленческих решений как в тактическом, так и в стратегическом аспектах.

Конкурентная разведка направлена на повышение конкурентоспособности хозяйствующего субъекта, что в конечном итоге должно приводить к максимизации прибыли коммерческого предприятия (организации). Следовательно, под конкурентной разведкой можно понимать особый вид предпринимательской деятельности, направленной на информационное обеспечение управления предприятием (организацией) с целью повышения его конкурентоспособности. Именно в этой трактовке конкурентная разведка выступает как экономическая категория.

Стратегическое предназначение конкурентной разведки заключается в необходимости обеспечивать постоянное соответствие между стратегией производственно-сбытовой деятельности хозяйствующего субъекта, действиями, с помощью которых эта стратегия реализуется, и состоянием постоянно меняющегося внешней рыночной среды.

Российское Общество профессионалов конкурентной разведки формулирует цель конкурентной разведки как глубокое понимание бизнеса в целом и отдельных его частей. Конкретизация **целей конкурентной разведки** на предприятии (в организации) представлены на рис. 1.

В цели конкурентной разведки входит только сбор соответствующей рыночной (маркетинговой) информации, а не ее анализ, являющийся в

данном случае только инструментом извлечения этой информации из косвенных данных в условиях недоступности прямых данных.

Рис.1. Цели конкурентной разведки

Задачи конкурентной разведки можно рассматривать как вспомогательную информационную функцию маркетингового анализа для целей стратегического управления предприятием (организацией).

Основными стратегическими задачами конкурентной разведки можно считать:

- определение сильных сторон каждого из основных конкурентов предприятия (организации), в частности – их основного уникального торгового предложения;
- определение ценовой политики конкурентов;
- определение методов продвижения на рынок конкурентных товаров и услуг;

- определение трендовой модели развития конкурентов на целевых рынках;
- определение круга реальных совокупных конкурентных преимуществ основных игроков на товарном (территориальном, отраслевом) рынках;
- определение перечня основных недостатков (слабостей) основных конкурентов;
- определение перечня партнёров – поставщиков основных конкурентов предприятия (организации), а также - условий их взаимного сотрудничества;
- определение перечня партнёров – покупателей основных конкурентов предприятия (организации), а также - условий их взаимного сотрудничества;
- определение перечня инфраструктурных (сервисных) партнёров основных конкурентов предприятия (организации), а также - условий их взаимного сотрудничества;
- определение состава ключевых партнёров (контрагентов), составляющих релевантную среду основных конкурентов предприятия (организации);
- определение состава определяющих должностных лиц и их реального статуса у основных конкурентов предприятия (организации);
- определение внешних ключевых фигур поддержки у основных конкурентов предприятия (организации), а также степень их связи с конкурентами;
- определение источников текущего финансирования основных конкурентов предприятия (организации);
- оценка инвестиционных финансовых ресурсов основных конкурентов предприятия (организации);
- определение структуры доходов по видам товаров (услуг) у основных конкурентов предприятия (организации);
- определение структуры расходов по видам деятельности и продуктам в конкурентной организации;
- определение рентабельности видов деятельности или продуктов в конкурентной организации;
- определение экономического механизма создания добавочной стоимости у основных конкурентов предприятия (организации), а также структуры их добавочной стоимости (затрат на производство и реализацию продукции);
- определение структуры бизнес-процессов формирования реализационных финансовых потоков у основных конкурентов предприятия (организации) в разрезе их процедурного воплощения;

• определение планов технического развития основных конкурентов предприятия (организации), в частности – их продуктового (товарного) портфеля.

Тактические задачи конкурентной разведки представлены на рис.2.

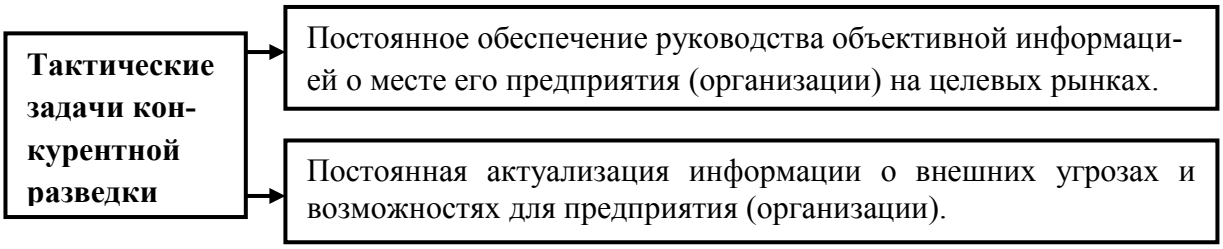

Рис. 2. Тактические задачи конкурентной разведки

Функции конкурентной разведки:

• изучение деятельности конкурентов и конкурентной среды предприятия (организации);

• проверка надежности деловых партнеров;

• сбор информации в сети Интернет, её постоянная актуализация, а также мониторинг материалов в средствах массовой информации (СМИ);

• исследование и анализ совместно с другими службами предприятия (организации), товарных (отраслевых) рынков или территорий (регионов);

• прогнозирование изменения ситуации на рынке и последующих потенциальных действий основных конкурентов предприятия (организации);

• выявление новых или потенциальных конкурентов предприятия (организации);

• оказания помощи руководству предприятия (организации) в процессе заимствования положительного опыта других хозяйствующих субъектов;

• оказание помощи специалистам прочих управленческих (производственных) подразделений предприятия (организации) в оценке целесообразности открытия нового направления деятельности (новой бизнес-единицы);

• получение законным путем информации о новых технологиях, товарах (услугах) или процессах, способных существенно повлиять на результаты производственно-сбытовой деятельности предприятия (организации), а её анализ и постоянная актуализация;

• выявление сильных и слабых сторон основных конкурентов предприятия (организации);

• совместно со службой экономической безопасности выявлять потенциальные источники утечки конфиденциальной информации внутри предприятия (организации).

Сегодня конкурентная разведка - инструмент менеджмента, позволяющий знать реальное рыночное положение предприятия (организации) и прогнозировать это положение в кратко, средне и долгосрочном периодах, что, в свою очередь, значительно повышает устойчивость хозяйствующего субъекта на товарных рынках.

Цели создания службы конкурентной разведки на предприятии (в организации) см. на рис. 3.

Рис.3. Цели создания службы конкурентной разведки предприятия (организации)

Задачи службы конкурентной разведки предприятия (организации):

- регулярный сбор информации о наиболее опасных конкурентах предприятия (организации): их рыночных долях, стратегиях, планах, взаимоотношениях с партнерами, поставщиками, потребителями;
- обработка и анализ собранной информации;
- своевременное информирование должностных лиц, принимающих управленческие решения, об изменениях на товарных (региональных, отраслевых, национальных) рынках, открывающихся рыночных возможностях и возникающих угрозах и т.п.;
- разработка предложений об улучшении организации отношений предприятия (организации) со своими партнерами и контрагентами;
- обеспечение (ограничение) доступа должностных лиц к соответствующей информации в соответствии с внутренним регламентом предприятия (организации).

Принципы работы службы конкурентной разведки предприятия (организации):

- целевая направленность: четкая и однозначно трактуемая работниками службы конкурентной разведки постановка целей сбора и анализа информации;

- полнота: сбор необходимой информации специалисты службы конкурентной разведки проводят, изучая все (любые) доступные источники;
- достоверность: для всей собранной рыночной информации специалисты службы конкурентной разведки определяют степень её достоверности;
- прогнозируемость: полученная в ходе проведения разведывательных мероприятий информация должна предоставлять возможность определения тенденций развития интересующих предприятие (организацию) рыночных процессов;
- постоянство: разведывательная работа осуществляется на постоянной основе, параллельно с созданием банка данных о наиболее значимых программах, мероприятиях и т. п., реализованных отдельными конкурентами предприятия (организации);
- изменяемость: постоянное отслеживание специалистами службы конкурентной разведки существенных изменений, происходящих в производственно-сбытовой деятельности наиболее опасных конкурентов, а также в макросреде предприятия (организации);
- разумная достаточность: в ходе своей профессиональной деятельности специалисты службы конкурентной разведки минимизируют сбор «нецелевой» информации для недопущения чрезмерного многообразия информационных потоков;
- общность: все специалисты службы конкурентной разведки предприятия (организации) применяют одинаковый терминологический аппарат при сборе и анализе информации;
- доступность: специалисты службы конкурентной разведки предприятия (организации) используют все доступные информационные источники, в том числе для перепроверки информации, путём раскрытия содержания полученных данных и их сопоставления с данными прошлых лет (данными других организаций);
- познаваемость: при работе с информационными массивами специалисты службы конкурентной разведки предприятия (организации) устанавливают причинно-следственные зависимости у исследуемых явлений;
- учет особенностей: при работе с информационными массивами специалисты службы конкурентной разведки предприятия (организации) учитывают национальные, социальные, экологические и иные особенности исследуемых явлений (разведывательной информации);
- наступательность: предлагаемые руководству специалистами службы конкурентной разведки ответные решения на реализуемые конкурентами рыночные программы (мероприятия) должны носить преимущественно наступательный характер;
- своевременность: специалисты службы конкурентной разведки должны своевременно предоставлять руководящему составу предприятия

(организации) и ведущим менеджерам целевой информации об основных конкурентах;

- уменьшающаяся ценность (полезность): учет специалистами службы конкурентной разведки в своей работе феномена падения во времени ценности (актуальности) собранной информации о конкурентах без её постоянной актуализации.

Направления работы службы конкурентной разведки предприятия (организации)представлены на рис. 4.

Рис. 4. Направления работы службы конкурентной разведки предприятия (организации).

Результатами работы службы конкурентной разведки предприятия (организации) следует считать**:**

- прогнозы потенциальных изменений на рынке;
- прогноз потенциальных действий основных конкурентов предприятия (организации);
- своевременное выявление новых или потенциальных конкурентов предприятия (организации) на целевых рынках;
- предоставление руководству и сотрудникам предприятия (организации) информации об ошибках или успехах других хозяйствующих субъектов, сопровождающих текущую и стратегическую рыночную деятельность последних;
- информационные данные мониторинга патентно-лицензионной ситуации на целевых для предприятия (организации) рынках;
- конкурентная (рыночная) оценка целесообразности для предприятия (организации) открытия нового подразделения или направления деятельности, а также – приобретения новой бизнес-единицы;
- постоянная актуализация информации о новых технологиях, товарах и услугах, появление (распространение) которых на целевых рынках может изменить существующее рыночное положение предприятия (организации);
- постоянная актуализация информации о политических, законодательных, регуляторных и т.п. изменениях на соответствующих рынках,

способных повлиять на существующее рыночное положение предприятия (организации);

- своевременная формулировка предложений в адрес руководства предприятия (организации) о необходимости (целесообразности) реализации той или иной бизнес-идеи;
- предоставление руководству информации о имиджевой репутации предприятия (организации) на целевых рынках с точки зрения ведущих рыночных игроков (партнёров, клиентов, конкурентов), а также властных, контрольных и правовых структур;
- разработка методических и инструктивных материалов по вопросам возможности применения на предприятии (в организации) современного инструментария менеджмента (маркетинга);
- участие совместно с руководителями предприятия (организации) и соответствующими структурными подразделениями в работе по ликвидации слабостей бизнеса и наращиванию его конкурентных преимуществ, как абсолютных, так и относительных (в сравнении с основными конкурентами);
- мониторинговая диагностика изменений на целевых рынках и обеспечение своевременной реакции на них предприятия (организации);
- выявление потенциальных источников утечки конфиденциальной информации через сотрудников предприятия (организации);
- диагностика сильных и слабых сторон в производственно-сбытовой деятельности основных конкурентов;
- сбор и постоянная актуализация информации о производственно-сбытовой деятельности партнеров и клиентов (потребителей продукции) предприятия (организации).

Служба конкурентной разведки не должна рассматриваться как частный случай безопасности предприятия. Сферой деятельности и объектами исследования службы конкурентной разведки предприятия (организации) являются только внешние риски, возможности и угрозы, имеющие исключительно рыночный характер и влияющие на возможности достижения хозяйствующим субъектом намеченных стратегических целей. Сферой деятельности и объектами исследований службы безопасности предприятия (организации) являются как внешние, так и внутренние риски и угрозы текущей деятельности хозяйствующего субъекта, имеющие, в том числе, криминальный характер и нарушающие его нормальную текущую производственно-сбытовую деятельность (табл. 1).

Таблица 1

Сравнительная характеристика деятельности подразделений конкурентной разведки в области стратегического менеджмента и в области безопасности предприятия (организации)

Принцип сравнения	Конкурентная разведка как часть стратегического управления предприятиям	Конкурентная разведка как часть системы безопасности предприятия
Субъект выполнения функций разведки	В крупных предприятиях – отдельное подразделение, в небольших один или несколько сотрудников из числа наиболее опытных специалистов в соответствующей отрасли бизнеса.	Подразделение или сотрудник в составе службы безопасности. Сотрудники: юристы, бывшие сотрудники правоохранительных органов.
Законодательные нормы работы	Рамки Гражданского кодекса РФ, т.к. используют только законные (напрямую не запрещенные) методы работы.	Рамки закона РФ № 2487-1 «О частной детективной и охранной деятельности в Российской Федерации» от 11 марта 1992 года.
Объект исследований (разведки)	Особо опасные с позиций стратегического менеджмента риски, угрозы и возможности внешней среды, поиск новых товарных рынков, рыночных ниш, направлений деятельности предприятия, каналов сбыта, внутренние информационные потоки.	Прямые угрозы и риски нормальной производственно-сбытовой деятельности предприятия или порчу его имущества (мошенничество, аферы, хищения, промышленный шпионаж, черный PR и т.п.).
Основные функции	Участие в комплексном управлении стратегическими и тактическими внешними рисками, информационное обеспечение процедуры принятия управленческих решений (сбор, обработка, хранение, предоставление информации).	Исполняет функцию обеспечения физической и экономической безопасности компании (в компании)
Источники информации	Поиск необходимых открытых и закрытых источников информации, фиксация начальных информационных сигналов, мониторинг информационной среды и актуализация корпоративных банков данных.	Работа с открытой информацией по сбору сведений о конкурентах и партнерах для подготовки к переговорам, для проверки криминальности контрагентов, сотрудников и т.д.
Цели и задачи	Информационно и аналитически обеспечивает достижение стратегических целей предприятия, в том числе – его конкурентных преимуществ на товарных рынках, а также обеспечивает управление информационными потоками о предприятии во внешней среде.	Обеспечивает защиту от прямых криминальных посягательств на стабильную работу предприятия.

1.2. Законодательное регулирование конкурентной разведки в РФ

Отличительная черта конкурентной разведки – это деятельность её сотрудников исключительно в правовом поле (национальном и международном).

Поэтому в своей работе специалист службы конкурентной разведке должен учитывать законодательные ограничители, изложенные в следующих правовых актах Российской Федерации:

- Уголовный кодекс Российской Федерации:
  - Статья 183 «Незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну»;
  - Статья 137 «Нарушение неприкосновенности частной жизни»;
  - Статья 138 «Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений»;
  - Статья 146 «Нарушение авторских и смежных прав»;
  - Статья 147 «Нарушение изобретательских и патентных прав»;
  - Статья 158 «Кража»;
  - Статья 159 «Мошенничество»;
  - Статья 163 «Вымогательство»;
  - Статья 189 «Незаконные экспорт из Российской Федерации или передача сырья, материалов, оборудования, технологий, научно-технической информации, незаконное выполнение работ (оказание услуг), которые могут быть использованы при создании оружия массового поражения, вооружения и военной техники»;
  - Статья 201 «Злоупотребление полномочиями»;
  - Статья 203 «Превышение полномочий служащими частных охранных или детективных служб»;
  - Статья 291 «Дача взятки»;
  - Статья 204 «Коммерческий подкуп»;
  - Статья 210 «Организация преступного сообщества (преступной организации) или участие в нем (ней)»;
  - Статья 128.1 «Клевета»;
  - Статья 275 «Государственная измена»;
- Федеральный закон «О персональных данных» от 27.07.2006 N 152-ФЗ;
- Закон РФ от 21.07.1993 N 5485-1 (ред. от 08.03.2015) «О государственной тайне»;
- Федеральный закон «О коммерческой тайне» от 29.07.2004 N 98-ФЗ;
- Гражданский Кодекс РФ;
- Федеральный закон «Об оперативно-розыскной деятельности» от 12.08.1995 N 144-ФЗ;

- законодательная и правоприменительная практика других стран.

От способа получения информации зависит, можно ли рассматривать эту информации как законную. Если можно доказать, что те или иные сведения получены законным путем и методами конкурентной разведки, то это означает, что данные сведения не были защищены достаточным образом. Следовательно, сам орган, призванный в служебном порядке защищать соответствующую информацию, допустил её сознательную или неосознанную утечку.

Законными методами получения информации в ходе работы сотрудников службы конкурентной разведки являются:

- наблюдение;
- опрос (беседа с людьми);
- сбор образцов.

Доступ к некоторой информации ограничивается с точки зрения круга лиц, которые имеют право в ходе выполнения своих служебных обязанностей знакомиться с ней с целью дальнейшего использования, так как её раскрытие может нанести ущерб государству, предприятию (организации), или же эта информация является персональными данными гражданина.

Поэтому во избежание случайного несанкционированного раскрытия государственной тайны гражданским специалистам не целесообразно заниматься сбором информации по вопросам военного характера и технологий двойного назначения. Сбор информации о личной жизни граждан незаконен, за исключением случаев, когда сотрудник службы конкурентной разведки обладает разрешением гражданина, в отношении которого осуществляется поиск конфиденциальной информации, или санкцией соответствующего органа государственной власти.

Уголовный кодекс (УК) РФ **запрещает** методы получения информации специалистами в области конкурентной разведки, перечисленные ниже:

– подкуп лиц, способных передать документацию по интересующей тематике либо образцы продукции (ст. 204 «Коммерческий подкуп», ст. 291 «Дача взятки» УК РФ);

– шантаж вышеназванных лиц (ст. 163 «Вымогательство» УК РФ);

– несанкционированное получение информации при помощи электронных устройств или технических средств снятия информации (ч. 2 ст. 138 «Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений» УК РФ, возможно также ч. 1 ст. 183 УК РФ - собирание сведений, составляющих коммерческую тайну);

– подслушивание деловых и личных телефонных и иных переговоров руководителей компании-конкурента, осуществление наружного наблюдения за ними (ч. 1 ст. 138 УК РФ - нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений);

– внедрение или вербовка агента для содействия в получении секретной либо компрометирующей гражданина или предприятие (организацию) информации (ст. 183 «Незаконные получение и разглашение сведений, составляющих коммерческую тайну» УК РФ);

– хищение документов или продукции конкурента (ст. 158 «Кража» либо ч. 1 ст. 325 УК РФ - похищение или повреждение документов, штампов, печатей либо похищение марок акцизного сбора, специальных марок или знаков соответствия);

– тайное проникновение на объект конкурента с целью изучения обстановки на его предприятии (в организации) (ч. 1 ст. 330 «Самоуправство»);

– диверсия, т.е. временный или постоянный вывод из строя образцов продукции, людей или предприятий (организаций) конкурента (ст. 167 «Умышленные уничтожение или повреждение имущества» УК РФ, ст. 111, 112 или 115 - умышленное причинение, соответственно, тяжкого, средней тяжести либо легкого время здоровью; ст. 281 «Диверсия», ч. 2. ст. 158 УК РФ - кража, совершенная с незаконным проникновением в помещение либо иное хранилище).

Категории информации ограниченного доступа представлены на рис. 5.

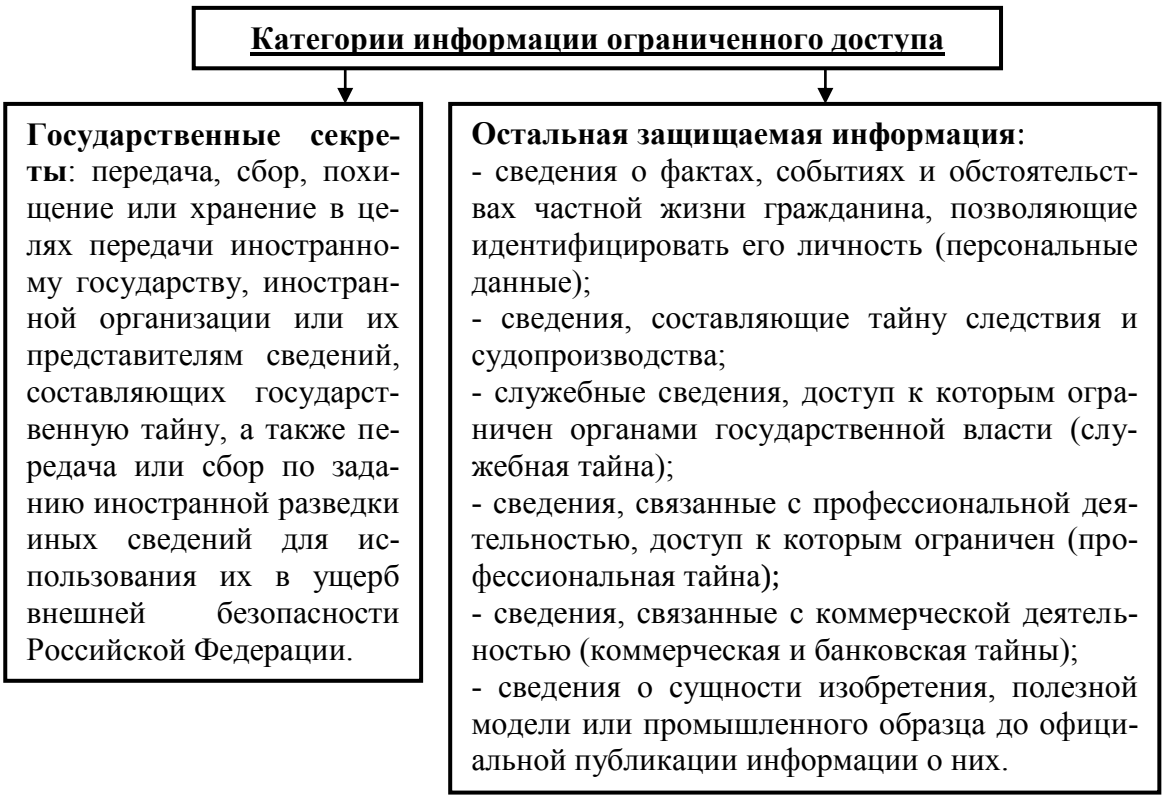

Рис. 5. Категории информации ограниченного доступа
и их краткая характеристика

Считается допустимым «вычисление» специалистами по конкурентной разведке данных, входящих в состав закрытой информации, путём анализа информации из открытых источников.

Промышленный шпионаж – форма недобросовестной конкуренции, при которой осуществляется незаконное получение, использование, разглашение информации, составляющей государственную, коммерческую, служебную или иную охраняемую законом тайну с целью получения третьим лицом преимуществ при осуществлении собственной предпринимательской деятельности, а также получения им материальной выгоды.

Основа промышленного шпионажа как вида деятельности – добывание и последующее использование коммерческой или служебной тайны сторонних субъектов рынка.

Методы промышленного шпионажа:

- подкуп или шантаж лиц, имеющих доступ к секретной информации;
- кража различных носителей с интересующими сведеньями;
- внедрение агента в конкурирующую фирму с целью получения информации, являющуюся её коммерческой или банковской тайной;
- осуществление незаконного доступа к коммерчески значимой информации конкурента с помощью использования технических средств (прослушивание телефонных линий, незаконное проникновение в компьютерные сети и т.п.);
- использование профессиональных психологов-манипуляторов для извлечения полезной информации у граждан, являющимися служащими конкурирующей фирмы;
- проведение замаскированных и ложных опросов граждан, являющихся служащими конкурирующей фирмы.

Направления борьбы с промышленным шпионажем со стороны конкурирующих фирм на предприятии (в организации):

– разграничение допуска сотрудников предприятия (организации) к охраняемой информации; запрет доступа к ней сотрудникам, которым для выполнения должностных обязанностей данная информация не нужна;

– обеспечение полной безопасности корпоративных компьютерных систем и сетей, создание собственной системы безопасности:

- ➢ контролирующей техническую безопасность служебных помещений (обеспечения отсутствия в них «жучков», скрытых камер и прочих приспособлений сбора информации);
- ➢ проводящей скрытое наблюдение за сотрудниками компании;
- ➢ совершенствующей инженерные и строительные конструкции, не соответствующие политике безопасности (например, устройство эффективной звукоизоляции в комнате переговоров).

2. ИНФОРМАЦИЯ В КОНКУРЕНТНОЙ РАЗВЕДКЕ

2.1. Общая характеристика информации в бизнесе

Информация — представленные в том или ином виде сведения, которые в процессе коммуникации воспринимаются человеком или специальными устройствами как отражение фактов материального мира.

Информация — знания о предметах, фактах, идеях и т. д., которыми могут обмениваться люди (информационно-передающие устройства) в рамках конкретного контекста.

Информация — знания относительно фактов, событий, вещей, идей и понятий, которые в определённом контексте имеют конкретный смысл.

Характеристика общих свойств информации представлена на рис. 6.

Рис. 6. Характеристика общих свойств информации

Основные з**аконы информации,** особенности действия которых необходимо учитывать в своей работе специалистам службы конкурентной разведки предприятия (организации), перечислены ниже.

Закон согласованных каналов информационного взаимодействия: системы или объекты могут обмениваться информацией только через согласованные каналы (например, печатные и виртуальные средства массовой информации обладают согласованными каналами обмена информацией внутри себя, но по отношению друг к другу их информационные каналы не согласованы).

Закон тезауруса: для адекватного восприятия информации объект её получения должен иметь соответствующий тезаурус для дешифрования и

усвоения поступающих сообщений. Тезáурус – особая разновидность словарей, в которых указаны семантические отношения (синонимы, антонимы, паронимы, гипонимы, гиперонимы и т.п.) между лексическими единицами. В отличие от толкового словаря, тезаурус позволяет выявить смысл не только с помощью определения, но и посредством соотнесения слова с другими понятиями и их группами (например, с помощью тезауруса можно изменить восприятие неподготовленным читателем сленговых, устаревших выражений, вышедших из постоянного употребления аббревиатур и т.п.). Лексическая единица – слово, устойчивое словосочетание или другая единица языка, способная обозначать предметы, явления, их признаки и т.п.

Закон фасцинации: чем более с точки зрения получателя эмоционально окрашена форма донесения информации, тем выше вероятность того, что он ее запомнит (обратит на неё внимание). Фасцинация – привлекательная для получателя форма донесения информации.

Закон майевтики: в некоторых случаях новая информация может не появляться извне, а быть результатом переработки уже имеющейся информации. Майевтика – искусство извлекать скрытое в человеке правильное знание с помощью искусных вопросов и ответов.

Закон перехода информации: информация в ходе работы с ней может превращаться в другую информацию (например, при интерпретации обрывков фраз, вырванных из контекста либо неправильно понятых).

Закон опосредованного управления: информация может быть использована в качестве «агента» опосредованного управления неким объектом (например, публикация в СМИ о зафиксированном росте цен на некоторые продукты питания способна спровоцировать ажиотажный спрос на эти товары, хотя соответствующие статьи не содержат никаких прямых управляющих посылов к упомянутым действиям со стороны объекта информационного воздействия).

Особенности восприятия информации её получателем (объектом восприятия) представлены на рис.7.

Рис. 7. Характеристика особенностей восприятия информации её получателем

Информация используется получателем (потребителем) для удовлетворения своих экономических и институциональных потребностей, а значит, является экономическим и институциональным благом.

Классификация информационных благ представлена на рис. 8:

Рис. 8. Общая классификация информационных благ

На современных предприятиях (в организациях) информационные блага рассматриваются как информационный ресурс наряду с природными ресурсами, трудом, капиталом и предпринимательской активностью.

Информация как ресурс обладает как общими с другими ресурсами, так и специфическими свойствами.

Общие свойства информации как ресурса:

- ограниченность, дефицитность, недостаточность для удовлетворения всех имеющихся потребностей;
- взаимозаменяемость;

- мобильность.

Специфические свойства информации как ресурса:

- сохранение объема информации в процессе использования;
- отсутствие зависимости между исходным объемом знаний и объемом нового созданного знания;
- способность информации координировать использование (наличие, объём) других ресурсов.

В состав **информационных благ**, используемых для удовлетворения потребностей лиц, входящих во внутреннее и внешнее окружение фирмы, включаются:

- услуги по предоставлению доступа к информации;
- информационные каналы;
- источники информации;
- программное обеспечение для работы с информацией и её источниками.

2.2. Информация в конкурентной разведке

В конкурентной разведке информация является результатом деятельности этой службы на предприятии (в организации). Следовательно, любые профессиональные действия (мероприятия), проводимые специалистами службы конкурентной разведки должны проводиться исключительно с целью получения новой информации или актуализации уже имеющейся информации.

Данные – первичный, исходный ресурс получения информации, основанные на фактах. Данные могут быть представлены в виде статистических данных, отрывочных сведений об интересующем объекте и т.д., как правило, не систематизированные в соответствии с требованиями стоящих перед конкурентной разведкой задач.

Информация – совокупность данных, снимающих или уменьшающих существующую до их получения неопределенность совокупности сведений об интересующем объекте, т.е. информация пригодна для принятия управленческого решения, являясь обработанной, проанализированной совокупностью данных. Например, в своем обычном виде бухгалтерский баланс предприятия (организации) является данными, а его (её) агрегированный бухгалтерский баланс может рассматриваться в качестве исходных данных для соответствующей аналитической работы.

Стандартный алгоритм формирования информации службой конкурентной разведки состоит из 5 этапов.

1 этап. Планирование и постановка целей. На данном этапе должны быть четко сформулированы цели проведения службой конкурентной разведки соответствующего мероприятия, определены корпоративные приоритеты, выбраны методы и средства сбора данных, установлены их

сроки, периодичность, назначены ответственные исполнители, а также форма, в которой собранные данные должны быть представлены для дальнейшей обработки.

2 этап. **Сбор и получение первичных данных**. На данном этапе осуществляется поиск источников данных и, при необходимости, - корректировка методов их сбора. Определяется, какой инструментарий доступен при поиске и сборе первичных данных в зависимости от широты диапазона вопросов и специфики поля поисков. На данном этапе необходим как можно более широкий охват независимых источников.

3 этап. Систематизация и обработка данных. В ходе данного этапа проводится систематизация полученных разрозненных данных, например, занесение их в базы данных, сводные таблицы и т.д. На данном этапе используются аналитические методы работы с данными, аналогичные методам анализа проблем и принятия управленческих решений.

4 этап. Анализ и синтез информации. На данном этапе данные преобразуются в информацию по следующему алгоритму:

– шаг 1: изучение систематизированных данных;

– шаг 2: анализ изученных данных;

– шаг 3: обобщение результатов анализа;

– шаг 4: формулирование выводов и выработка рекомендаций.

При невозможности получения однозначных выводов специалисты службы конкурентной разведки прибегают либо к построению гипотез, либо к повторному проведению предшествующих этапов. На данном этапе проводится концентрация данных в едином аналитическом центре, проводится полный цикл их систематизации и преобразование данных в информацию.

5 этап. Распространение информации. На данном этапе проводится знакомство «заказчиков» информации с результатами проведенной работы. Распространение сформированной информации должно проводиться по оговоренным на первом этапе каналам и среди определенного круга лиц, т. к. часто полученная информация является стратегически важной и нуждается в корпоративной защите в качестве легко копируемого конкурентного преимущества.

Типы источников информации представлены на рис.9.

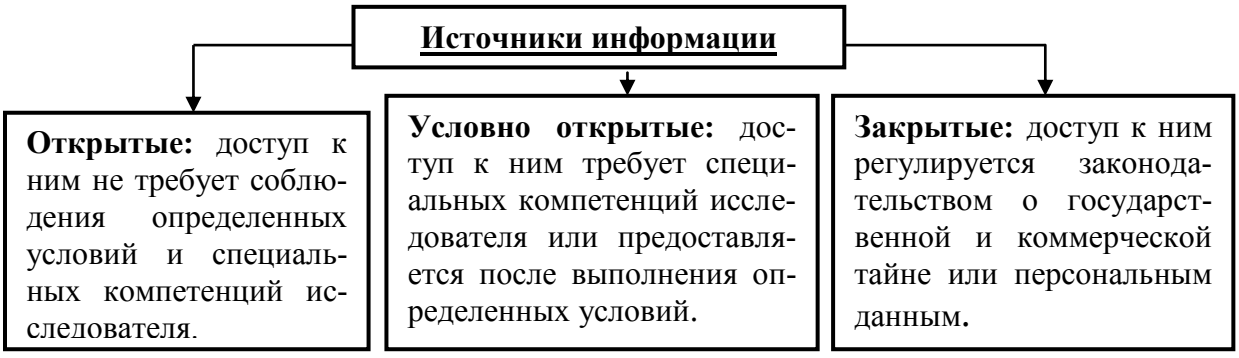

Рис. 9. Типы источников информации

Классификация коммерческой информации

- **По отношению к решаемым задачам**:
  - стратегическая информация: информация о глобальных процессах экономики или интересующего региона, техники и технологии, НИОКР и т. д.;
  - тактическая информация: информация, необходимая для принятия текущих управленческих решений.
- **По степени объективности и достоверности;**
- **По источнику получения**:
  - по степени открытости (закрытые, условно открытые и открытые);
  - по отношению к предприятию (организации), проводящему сбор информации (внутренние и внешние);
  - по субъекту предоставления информации (источники органов власти и местного самоуправления, некоммерческих организаций, коммерческих организаций, частных лиц);
  - по уникальности (оригиналы (копии), выдержки, фрагменты, заимствования);
  - по физической природе (люди, вещи и документы).
- **По степени открытости**:
  - открытая;
  - закрытая.

Наиболее часто служба конкурентной разведки предприятия (организации) проводит сбор коммерчески важной информации в рамках изучения производственно-сбытовой деятельности фирмы – конкурента. Данная работа проводится по двум направлениям: получение общей информации о хозяйствующем субъекте, содержащейся в различных регистрационных и справочных источниках, и получение специальной (неофициальной) информации.

В состав о**бщей информации** о хозяйствующем субъекте включаются следующие данные**:**

- установленные данные о юридическом лице;
- полное наименование предприятия (организации) и виды деятельности.
- организационно-правовая форма предприятия (организации): место, дата и номер государственной регистрации;
- юридический и фактический адрес предприятия (организации), контактные телефоны и электронные адреса;
- название и адрес банка, в котором обслуживается предприятие (организации), номера банковских счетов и их баланс;
- уставный капитал, информация об учредителях, названия (имена) учредителей, величина их учредительских долей;

- информация о руководящих должностных лицах предприятия (организации): директоре, его заместителях, главном бухгалтере, их профессиональной биографии, о работе на других предприятиях, их домашние адреса, контактные телефоны и т.п.;
- наличие у предприятия (организации) лицензий на определенные виды деятельности.

В состав **специальной информации** о хозяйствующем субъекте включаются следующие данные**:**

- отношения предприятия (организации) с властями: характерные события, конфликты, доверительные контакты, степень использования административного ресурса, отношение чиновников к хозяйствующему субъекту в сравнении с другими;
- связи сотрудников предприятия (организации) с криминальными структурами: единичные или регулярные контакты, конфликты, степень близости;
- характеристика сотрудников, входящих в состав руководства предприятия (организации): профессиональная и морально-бытовая репутация, здоровье, владение собственностью, оружием, наличие судимости, арестов, участие в судебных процессах, наличия статуса учредителя или должностного лица на других предприятиях (в организации);
- особые события: перепродажа учредительской доли предприятия (организации), возврат или возникновение долгов, возбуждение уголовных дел в отношении сотрудников предприятия (организации), увольнение персонала, сопровождающееся исковыми заявлениями в суд и т.п.

Основные **источники** коммерческой информации представлены на рис. 10.

Рис. 10. Источники коммерческой информации для предприятия (организации)

Характеристика источников коммерческой информации представлена ниже.

Открытые источники коммерческой информации являются, как правило, общедоступными**.** К числу таких источников относятся средства массовой информации (газеты, журналы, альманахи, обзоры и т.п. как в традиционном, так и в электронном виде, публикации в интернете) и публичные событийные мероприятия (выставки, пресс-конференции и т.п.).

Разведывательный признак – это проявление активности исследуемого объекта, по которому можно судить о характере деятельности этого объекта. К косвенным разведывательным признаки, используемым в ходе конкурентной разведки, относятся результаты причинно-следственного анализа. Модель такого анализа представляет собой следующую логическую цепочку: рыночное явление «А» вытекает из рыночного явления «В», а рыночное явление «В» вытекает, в свою очередь, из рыночного явления «С». Следовательно, наблюдая «С», можно сделать некоторые выводы о «А». Причинно-следственный анализ является достаточно привлекательным и доступным методом получения коммерческой информации, однако он имеет ряд существенных **недостатков:**

- коммерческие связи между рыночными явлениями, определяемые специалистами службы конкурентной разведки предприятия (организации), а, следовательно, и сделанные на их анализе выводы всегда носят вероятностный характер;
- поскольку выявленные связи могут быть множественными, в ходе проведения анализа может возникнуть ситуация множественности гипотез или обратного эффекта;
- т.к. анализ проводится в условиях отсутствия проверенных данных, то в построении логических гипотез и связей могут появляться так называемые «черные дыры».

Оперативные данные – это результат проведенных оперативных мероприятий и разведывательных действий службой конкурентной разведки предприятия (организации). К получению данных (информации) оперативными методами специалисты прибегают при невозможности использования остальных методов, т.к. оперативная разведка является одним из наиболее сложных, затратных и рискованных методов получения коммерческой информации.

Экспертная оценка – это данные или уже готовая к использованию информация, полученная от особой группы источников – экспертов в интересующей профессиональной области. Работа с подобными данными (или информацией) требует от специалистов службы конкурентной разведки специальной подготовки (квалификации), т.к. в предоставленных им материалах практически невозможно отделить частное мнение эксперта от реальной ситуации в интересующей предприятие (организацию) облас-

ти. Следовательно, экспертная оценка всегда имеет субъективный характер. Для обеспечения максимальной эффективности получаемой из рассматриваемого источника коммерческой информации службе конкурентной разведки необходимо выбирать эксперта, удовлетворяющего следующим **основным требованиям**:

- высокий уровень профессионализма (профессиональных знаний) в интересующей предприятие (организацию) области;
- обладание опытом работы и профессиональными (деловыми) контактами, позволяющими ориентироваться в анализируемом вопросе и иметь возможность постоянной актуализации собственной квалификации;
- лояльное отношение к предприятию (организации).

Экспертная оценка может помочь не только получить конкретные данные (информацию), но и вывести на новый, до этого не рассматриваемый уровень сам процесс поиска источника данных.

Агентурные данные – это полученные от агентов сведения о фактах и лицах, представляющих интерес для службы конкурентной разведки предприятия (организации). При использовании данного источника коммерческой информации специалисты анализируют связи и возможные контакты всех персоналий, занимающих ключевые посты, а также части рядовых сотрудников предприятия (организации). Высшее руководство с большей вероятностью имеет тот или иной доступ к фирмам-конкурентам или в органы власти. Поэтому специалист в области конкурентной разведки обязан учитывать возможность получения от топ-менеджеров предприятия (организации) соответствующих данных (информации). Первоначальный отбор сотрудников, которых возможно использовать с целью получения агентурных данных, осуществляется по итогам анализа резюме и предыдущего опыта их работы. Итогом этого отбора является определение круга лиц, которым наиболее просто и эффективно поддерживать нужные службе конкурентной разведки контакты.

Материалы специализированных сторонних организаций (консалтинговых и аналитических агентств) могут использоваться (приобретаться) службой конкурентной разведки предприятия (организации) в случае, когда интерес представляет общедоступная информация (например, по политической, экономической, социальной ситуации в регионе.

Максимальный эффект от процесса получения коммерческих данных (коммерческой информации) достигается только при комплексном подходе, т.е. при использовании в ходе сбора этих данных (информации) одновременно из нескольких источников.

Качество информации – это степень пригодности конкретной информации для достижения поставленных «заказчиком» перед службой конкурентной разведки целей.

Качественные характеристики информации:

- **достоверность** – мера приближенности информации к первоисточнику или точность передачи данных;
- **объективность** – мера отражения информацией реальности;
- **однозначность** – отсутствие возможности многозначного толкования той или иной информации;
- **достоверность источника** – степень приближенности источника к месту зарождения информации;
- **порядок приближения** – количество звеньев между первоисточником информации и её конечным пользователем.

Количественные характеристики информации:

- **полнота информации** – степень достаточного соответствия полученной информации (данных, сведений) поставленным целям конкурентной разведки (полнота информации отражает отсутствие или наличие «информационных дыр» в полученных сведениях);
- **релевантность информации** – количественная характеристика, отражающая степень приближения информации к существу вопроса, степень соответствия полученной информации поставленным задачам.

Ценностные характеристики информации:

- **стоимость информации –** затраты на получение информации, её техническую и аналитическую обработку, хранение и передачу заказчику;
- **актуальность** (своевременность) **информации** – поступление информации в пределах времени, когда она полезна для принятия решений.

Критерии классификации методов получения информации в конкурентной разведке представлены на рис. 11.

Рис. 11. Критерии классификации методов получения информации в конкурентной разведке

Характеристика методов получения информации в конкурентной разведке представлена ниже.

Прямыми называются методы получения интересующей информации непосредственно из доступного источника. **Косвенными** методами называются способы вычисления интересующего показателя на основании значений других показателей, непосредственно связанных с ним. Большинст-

во методов конкурентной разведки является косвенными, так как косвенные данные об объекте более доступны, нежели прямые.

Наружным называется наблюдение за объектом конкурентной разведки без контакта с представителями интересующей стороны (например, конкурента). Любой способ получения информации, использующий контакты с сотрудниками организации-конкурента, связан с вторжением (проникновением) в нее. Большинство способов конкурентной разведки связано с получением информации от сотрудников компании - конкурента под каким-либо благовидным предлогом, более или менее распространенным в обычной деловой жизни. Проникновение специалисты службы конкурентной разведки предприятия (организации), как правило, осуществляют с привлечением к этому процессу либо сотрудников специализированных (консалтинговых) организаций, либо своих знакомых, включая друзей и родственников.

Кабинетные методы получения информации проводятся специалистами службы конкурентной разведки предприятия (организации) с целью сбора вторичной информации путём изучения данных, полученных из опубликованных источников. Вторичная информация — это информация, предварительно собранная другим лицом или для других целей, не связанных с текущим исследованием конкурентной среды. Кабинетные методы просты в использовании, как правило, недороги, отнимают мало времени и могут проводиться незаметно для объекта исследования. Полевые методы получения информации используются при работе с первичной информацией. Первичными называются исследования, связанные со сбором данных при их возникновении. Полевые методы позволяют получить более точную специальную информацию, изначально ориентированную на достижение целей, поставленных службой конкурентной разведки предприятия (организации). Однако их проведение требует больших финансовых и временных затрат. Поэтому на практике почти всегда кабинетные и полевые методы работы комбинируются специалистами конкурентной разведки друг с другом.

Виды кабинетных исследований (сбор информации из открытых источников):

- анализ рекламных обращений и открытых публикаций в средствах массовой информации, интернете и других открытых источников;
- посещение публичных выставок, отраслевых конференций и семинаров;
- оценка объема, структуры и стоимости рекламных расходов конкурентов исходя из рыночной стоимости проводимых ими маркетинговых мероприятий;
- сбор и анализ финансовых отчетов конкурентов на основании открытой информации государственных органов статистики;
- сбор и анализ отраслевых маркетинговых отчетов, публикуемых консалтинговыми организациями.

Законные виды первичных исследований (сбор закрытых сведений):

- опрос клиентов, общих для предприятия (организации) и его основных конкурентов;
- опрос поставщиков, общих для предприятия (организации) и его основных конкурентов;
- сбор сведений в ходе бесед (опросов) с бывшими сотрудниками предприятия (организации);
- сбор сведений в ходе бесед (опросов) с соискателями на замещение вакантных должностей на предприятии (в организации);
- сбор сведений в ходе бесед с сотрудниками предприятий (организаций), конкурирующих с основными конкурентами предприятия (организации), проводящего сбор информации;
- проведение сотрудниками службы конкурентной разведки незавершенной и завершенной пробной покупки;
- организация сотрудниками службы конкурентной разведки попытки сотрудничества или кооперации с объектом сбора информации от собственного имени предприятия (организации);
- организация сотрудниками службы конкурентной разведки попытки сотрудничества с объектом сбора информации под видом потенциального поставщика;
- организация сотрудниками службы конкурентной разведки попытки сотрудничества с объектом сбора информации под видром сервисного поставщика;
- опрос сотрудников конкурирующего хозяйствующего субъекта под видом проведения маркетингового исследования консалтинговой организацией;
- провокация сотрудника конкурирующего хозяйствующего субъекта адресным вопросом на форуме в интернете;
- сбор информации под видом соискателя на замещение вакантной должности на предприятии (в организации), являющемся объектом исследования сотрудниками службы конкурентной разведки;
- организация и поддержание знакомства с сотрудником конкурирующего хозяйствующего субъекта от третьего лица;
- использование для сбора информации анонимного интернет - знакомства с сотрудником конкурирующей организации;
- организация службой конкурентной разведки сотрудничества с объектом сбора информации под видом сервисного поставщика от лица третьей компании;
- организация сотрудниками службы конкурентной разведки попытки слияния хозяйствующих субъектов от собственного имени предприятия (организации);
- организация сотрудниками службы конкурентной разведки попытки инвестиций (полной или частичной покупки бизнеса конкурента) от третьего лица.

Незаконные виды первичных исследований (сбор закрытых сведений), нарушающие Законы «О коммерческой тайне», «О банковской деятельности», «О полиции», «О государственной службе», уголовный кодекс в части вторжения в частную личную жизнь, незаконного проникновение в помещение, незаконного доступа к информационным системам, превышения служебных полномочий, незаконной предпринимательской деятельности, а также преступлений, связанных с вербовкой (шантаж, угроза насилия, подкуп):

- использование личностных связей в государственных органах власти;
- использование личностных связей в правоохранительных органах;
- использование личностных связей в криминальной среде;
- использование личностных связей в банковской сфере;
- скрытное копирование данных информационной системы предприятий-конкурентов;
- скрытное проникновение в информационную систему конкурента;
- использование для сбора информации технических средств аудио, видео наблюдения;
- вербовка службой конкурентной разведки персонала предприятия-конкурента;
- тайное внедрение своего персонала в структуру организации-конкурента;
- использование для сбора информации существующего сексуального объекта конкурента;
- скрытное наружное наблюдение за контактами ключевых сотрудников предприятия-конкурента с целью сбора информации информации;
- организация сексуального контакта сотрудника конкурирующей организации с последующим использованием его в качестве информатора.

Информация признается достоверной, если соответствующие данные, полученные из нескольких (не менее двух) источников совпадают.

Организация изучения предприятий-конкурентов службой конкурентной разведки предприятия (организации), как правило, проводится по схеме, представленной на рис. 12.

Дезинформация – это способ воздействия на человека, путём предоставления ему информации, вводящей в заблуждение относительно истинного положения дел.

Цель распространения дезинформации – побуждение оппонента к поступкам, необходимым манипулятору: объект, в адрес которого направлена дезинформация, должен либо принять нужное манипулятору решение, либо отказаться от принятия решения, невыгодного для манипулятора. Таким образом, конечной целью создания и распространения дезинформации всегда является действие, которое будет предпринято оппонентом под её воздействием.

Виды дезинформации:

- введение в заблуждение конкретного лица или группы лиц, вплоть до целой нации;
- манипулирование поступками человека или группы лиц;
- создание общественного мнения относительно какой-то проблемы или объекта.

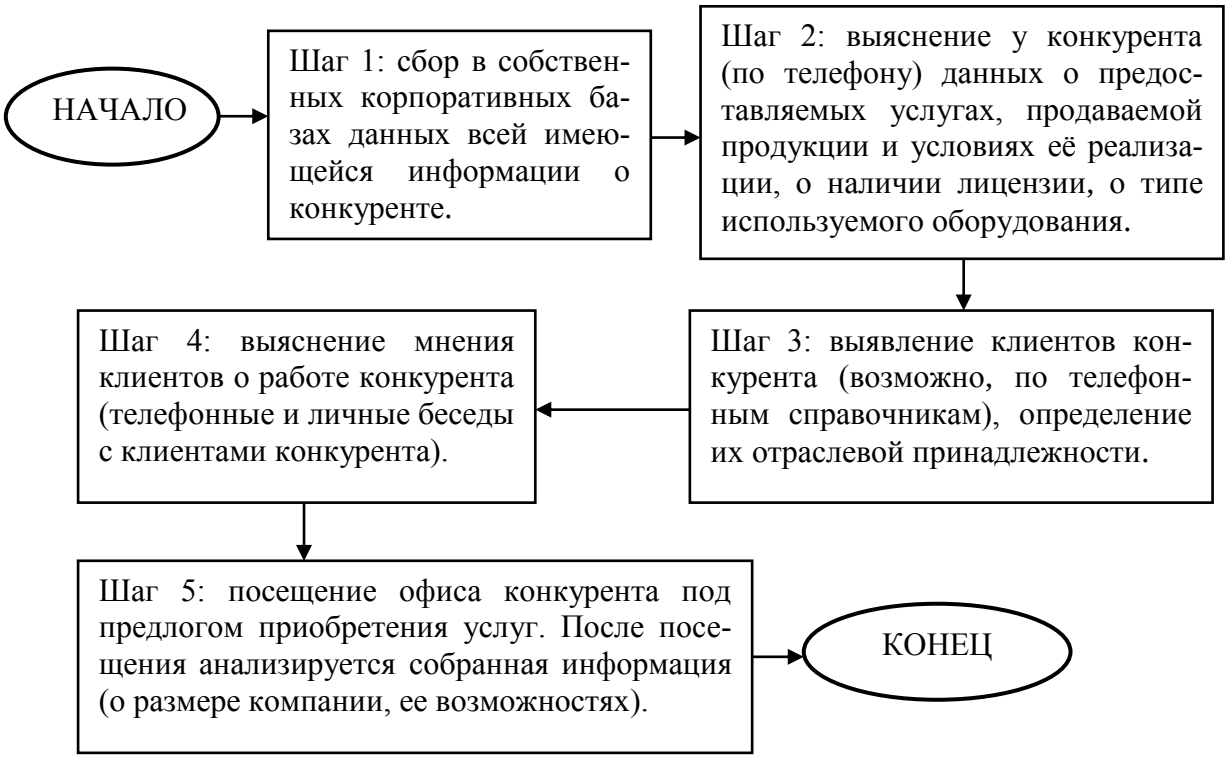

Рис. 12. Типовой алгоритм организации работы по изучению конкурентов

Введением в заблуждение называется прямой обман в виде предоставления объекту ложной информации.

Манипулирование называется способ воздействия на объект непосредственно с целью изменения направления активности людей. Уровни манипулирования:

- усиление существующих в сознании людей выгодных манипулятору ценностей (идей, установок…);
- частичное изменение взглядов людей на некоторое событие или обстоятельство;
- кардинальное изменение жизненных установок людей, являющихся объектами манипулирования.

Создание общественного мнения – это формирование в обществе определенного отношения к той или иной проблеме.

Задачи, решаемые службой конкурентной разведки с помощью адресного распространения дезинформации:

- введение в заблуждение конкурента относительно истинного времени начала тех или иных крупных мероприятий, проводимых предпри-

ятием (организацией) на рынке (например, начало продаж нового товара, проведение рекламной акции и т.п.);

➢ создание у конкурента иллюзии подготовки предприятием (организацией) крупномасштабных операций на ложном направлении (например, ложное объявление о намерение принимать участие в тендере).

Пути распространения дезинформации службой конкурентной разведки:

➢ широкое освещение от имени третьего лица в средствах массовой информации данных, свидетельствующих о появлении у предприятия (организации) «труднопреодолимых» проблем;

➢ организация «утечки» в СМИ и прочих открытых источниках информации заведомо заниженных или завышенных экономических и производственных показателей деятельности предприятия (организации);

➢ преувеличение или занижение отрицательного влияния климатических, бытовых, социальных и т. д. характеристик регионального (товарного) рынка на перспективность того или иного направления деятельности хозяйствующих субъектов;

➢ критика от имени третьего лица в средствах массовой информации данных «низкого качества» продукции, выпускаемой предприятием (организацией);

➢ значительное преувеличение в СМИ и прочих открытых источниках информации возможностей предприятия (организации): экономических, политических, социальных, административных и т.п.;

➢ публичная демонстрация службами предприятия (организации) серьезных производственно-сбытовых намерений на бизнес – направлении, которое, как известно специалистам конкурентной разведки, бесперспективно.

Основные приемы дезинформирования, применяемые службой конкурентной разведки предприятия (организации), представлены на рис. 13.

Рис. 13. Основные приемы дезинформирования, применяемые службой конкурентной разведки предприятия (организации)

Характеристика основных приемов дезинформирования, применяемых службой конкурентной разведки предприятия (организации), представлена ниже.

Информационная перегрузка: сообщение параллельно с основной информацией огромного количества вспомогательной, сопутствующей информации, представляющей собой абстрактные рассуждения, ненужные подробности, разнообразный информационный мусор, в результате чего объект воздействия оказывается не в состоянии разобраться в истинной сути проблемы.

Дозирование информации: сообщение целевой аудитории только выгодной части информации и замалчивание остальных данных. Результатом такого воздействия становится искажение в сознании оппонента реальной рыночной ситуации.

Стереотипизация: создание в сознании представителей целевой аудитории иллюзорных стереотипов (так называемых «ценностей»: стандартов поведения, социальных мифов, политических иллюзий и т.п.) и воздействие с их помощью на поведение целевой аудитории в целом.

Сенсация и сенсационность: использование информации о некотором исключительном с бытовой точки зрения событии, которое вызывает интерес широких масс, и о впечатлении, произведенном на общество этим событием, для отвлечения внимания этих масс от действительно важных рыночных событий (трендов, движений и т.п.).

Смешение (использование полуправды и инсинуаций): смешивание в информационных потоках истинных фактов с разнообразными слухами, гипотезами, допущениями, предположениями, рассуждениями до степени, когда оппоненту становится невозможно отличать правду от вымысла.

Большая ложь: использование для воздействия на представителей целевой аудитории психологического феномена: чем наглее и неправдоподобнее обман, тем скорее люди в него поверят.

Затягивание времени: оттягивание момента обнародования (предоставления) важных для представителей целевой аудитории сведений, например, о последствиях того или иного события до той поры, когда вследствие недостатка времени и ресурсов в наступающих событиях уже никому не возможно что-то изменить.

Замалчивание: намеренное замалчивание определенных фактов, недопущение распространения определенной информации аналогично тому, как это происходит при применении приема «затягивание времени».

Легализация информации: сообщение и распространение среди представителей целевой аудитории выгодной манипулятору информации (вымышленной или реальной) через подставных лиц или через нейтральные по отношению к манипулятору и объекту манипуляции средства массовой информации и другие открытые источники.

Своевременная ложь: сообщение представителям целевой аудитории ложной, но ожидаемой ими в настоящий момент информации. Чем сильнее ложь отражает ожидания аудитории, тем эффективнее оказывается результат от её распространения. Ко времени, когда обман будет раскрыт рыночными игроками, актуальность достоверной информации будет потеряна или важный для манипулятора рыночный процесс примет необратимый характер.

Информационные каналы наряду с источниками информации и программным обеспечением для сбора, хранения, обработки и распространения информации являются одной из групп информационных ресурсов. С их помощью предприятие (организация) работают с информацией (получает её и распространяет). К числу наиболее распространённых информационных каналов относятся следующие:

- интернет-ресурсы (сайты, форумы, блоги, электронные доски объявлений, социальные сети);
- пресса;
- радио;
- телевидение;
- выставки;
- конференции;
- семинары;
- обычная и электронная почта;
- юридические и физические лица;
- органы власти и местного самоуправления;
- вещи.

3. МЕТОДЫ РАБОТЫ В КОНКУРЕНТНОЙ РАЗВЕДКЕ

3.1. Работа со сторонними организациями

Служба конкурентной разведки предприятия (организации) должна широко пользоваться услугами сторонних организаций по доступу к информации, которая, являясь вторичной, позволяет достаточно дешево и быстро проводить предварительный анализ рыночной ситуации. Результаты этого анализа, в свою очередь, позволяют без снижения качества информации для принятия конечного управленческого решения отказаться от ряда более дорогостоящих первичных исследований определённой рыночной ситуации.

Ниже представлен перечень сторонних организаций, уставные (предписанные) виды деятельности которых позволяют использовать услуги, оказываемые ими, как с источники соответствующей информации.

Федеральная служба статистики (Росстат) осуществляет сбор, автоматизированную обработку, накопление, актуализацию, распространение информации. Главный межрегиональный центр обработки и распространения статистической информации Федеральной службы государственной статистики (ГМЦ Росстата) осуществляет следующие **виды деятельности**:

- сбор, контроль, обработку, накопление, хранение показателей государственной статистической отчетности, выпуск свободной статистической информации, формирование макроэкономических показателей, проведение балансовых расчетов, хранение и представление статистической и экономической информации, защита ее от несанкционированного доступа;
- издание и тиражирование докладов о социально-экономическом положении РФ, сводных и тематических статистических сборников, а также других официальных статистических публикаций и материалов Федеральной службы государственной статистики;
- распространение (в т.ч. на коммерческой основе) на территории России и за рубежом официально разрешенной статистической информации, проведение публикаций Федеральной службы государственной статистики;
- выполнение работы по созданию и ведению статистического регистра предприятий и организаций (Статрегистр), банка данных «Бухгалтерская отчетность организаций» (БД БОО), автоматизированного банка общероссийских классификаторов (АБК);
- создание, внедрение, ведение и актуализация статистических баз и банков данных, регистров, субрегистров, в т.ч. коммерческих;
- выполнение организационных, методологических и технологических работ по подготовке и проведению переписи населения, обработке её материалов, а также соответствующих единовременных обследований;

- проведение обработки материалов переписей и обследований, подготовка к публикации и распространение их итогов;
- обеспечение хранения материалов переписи населения на технических носителях, защита их от несанкционированного доступа, ведение информационных фондов на основе материалов переписи населения;
- формирование и ведение отраслевого фонда алгоритмов и программ Федеральной службы государственной статистики;
- осуществление информационно-технологического взаимодействия между территориальными органами Федеральной службы государственной статистики;
- координация работы по созданию и ведению общесистемных регистров, банков и баз данных территориальными органами и организациями Федеральной службы государственной статистики;
- присвоение кодов по общероссийским классификаторам технико-экономической и социальной информации юридическим лицам, их представительствам и филиалам, гражданам, занимающимся предпринимательской деятельностью без образования юридического лица, при их учете в составе ЕГРПО (Единый государственный регистр предприятий и организаций);
- осуществление взаимодействия с информационными системами и ресурсами министерств и ведомств;
- обеспечение сбора, обработки, хранения бухгалтерской отчетности организаций в составе БД БОО, формирование сводной информации по бухгалтерской отчетности для предоставления федеральным органам исполнительной власти;
- осуществление разработки и ведения общероссийских классификаторов технико-экономической и социальной информации;
- обеспечение автоматизированного ведения общероссийских классификаторов в рамках автоматизированного банка общероссийских классификаторов (АБК);
- распространение (в т.ч. на коммерческой основе) на территории России и за рубежом информации из Статрегистра, БД БОО, АБК.

Росстат также ведет статистический регистр хозяйствующих субъектов всех предприятий и организаций РФ, прошедших государственную регистрацию с ежемесячной актуализацией таких данных, как наименование, адрес, виды хозяйственной деятельности предприятия (организации), имя руководителя, состав учредителей.

Услуги, оказываемые учреждениями Статрегистра хозяйствующим субъектам, в том числе – на коммерческой основе:

- предоставление заказчику данных статистического учета по полному или предварительно отобранному составу показателей;
- составление по заявке заказчика выборки требуемых хозяйствующих субъектов по заданным критериям (наименование субъекта, виды

экономической деятельности, регионы, формы собственности и т.д.);

- предоставление заказчику адресной информации (наименование, местонахождение хозяйствующего субъекта, заявленное при регистрации, контактные линии, имя и должность руководителя);
- предоставление заказчику с последующим сопровождением тематических информационных фондов по заданным критериям (формирование информационного файла, содержащего набор требуемых хозяйствующих субъектов, по каждому из которых приведен согласованный перечень требуемых показателей).

Федеральная налоговая служба имеет право на основании сделанных в её адрес запросов предоставлять сведения о физических лицах (индивидуальных предпринимателях) и юридических лицах, т.к. в соответствии с российским законодательством сведения государственного реестра являются открытыми и общедоступными (за исключением паспортных данных и ИНН граждан).

Министерство иностранных дел РФ через специальный департамент экономического сотрудничества собирает открытую информацию о рыночной, политической, экономической, социальной ситуации в отдельных регионах мира, а также о конкретном предприятии, включая его кредитную историю, репутацию, сведения о финансовом положении и учредителях, которую в случае необходимости может получить сторонний заказчик информации.

Министерство внутренних дел РФ осуществляет обязательную проверку в реестре МВД всех граждан, с которыми заключаются контракты на управление юридическими лицами, создает специальные базы данных и ведет реестр «дисквалифицированных лиц». Данные из этой базы могут быть выданы по специальному запросу.

Федеральная служба судебных приставов может предоставить заинтересованным лицам информацию об арестованном имуществе и реестре должников.

Министерство экономического развития РФ может предоставить информацию по конкретному рыночному игроку, оно также составляет прогнозы экономического развития как страны в целом, так и отдельного региона.

Российские частные информационные агентства, работающие на рынке консалтинговых услуг, за счет большого объема информации, собственных корпоративных баз данных и т.п. могут предоставлять заказчику интересующую его конкретную информацию и давать экспертную оценку по отдельному запросу (например, по конкурирующей компании). Отличительной особенностью данных организаций является их долгосрочное сотрудничество с государственными информационными службами, детективными бюро, службами безопасности предприятий (организаций), что позволяет заказчикам приобретать у них экспертно достоверную информацию.

Иностранные консалтинговые фирмы и кредитные бюро (информационные системы, через которые кредиторы на постоянной основе обмениваются информацией о платежеспособности заемщиков) разрабатывают кредитные рейтинги заёмщиков. В основе этих рейтингов лежат сведения, которые кредиторы передают о своих заемщиках. Сведения собираются десятилетиями, а в некоторых случаях - сотнями лет. Кредитные бюро функционируют в большинстве развитых стран мира и торгуют имеющейся у них информацией о хозяйствующих субъектах.

Однако служба конкурентной разведки предприятия (организации) должна иметь в виду, что при обращении в консалтинговые фирмы или к независимому эксперту кроме возможности получения нужной информации существует риск утечки собственной конфиденциальной информации. Кроме того, некоторые консалтинговые фирмы, будучи официально независимыми, являются, по сути, внешними подразделениями конкурентной разведки крупных товаропроизводителей.

Офисы продаж, торговые точки, склады используются производителями в качестве независимых каналов продвижения своих товаров на рынок. В них размещаются образцы товаров, работают специалисты, консультирующие потенциальных покупателей о предлагаемой продукции и технологии ее изготовления, информирующие посетителей о проводимых товаропроизводителем рекламных мероприятиях, оформляющих заказы на поставку товаров. Одновременно все виды торговых представительств можно рассматривать как каналы получения информации для специалистов конкурентной разведки о существующих в конкурентных фирмах ценах, о предлагаемых скидках и способах доставки (продвижения) товаров и услуг, качестве обслуживания клиентов. Посещение торговых представительств – легальный способ знакомства с образцами предлагаемых конкурентом изделий и оценки материально-технической оснащенности его производственной базы. Наиболее популярным способом получения подобной информации является метод «Тайный покупатель», при котором исследователь представляется потенциальным клиентом и в процессе переговоров получает нужные сведения.

3.2. Документы как источник информации

К документам как к источникам интересной для службы конкурентной разведки предприятия (организации) информации о конкурирующих фирмах должны быть отнесены их учредительные документы, отчетность, техническая документация, рекламные материалы и публикации. Основные виды документов хозяйствующего субъекта, рассматриваемых службой конкурентной разведки в качестве потенциальных источников информации, представлены на рис. 14.

Рис. 14. Виды документов хозяйствующего субъекта – потенциальных источников информации для службы конкурентной разведки

Характеристика видов документации хозяйствующего субъекта, рассматриваемых службой конкурентной разведки в качестве потенциальных источников информации, представлена ниже.

Учредительные документы, квартальный и годовой бухгалтерские отчеты предприятий (организаций) составляют **группу легко формализуемых документов,** содержащих **достаточно достоверную информацию**, т.к. их состав определяется законом и рядом подзаконных актов.

Учредительные документы содержат следующую общую информацию о хозяйствующих субъектах:

- название;
- организационно-правовую форму;
- список учредителей;
- распределение учредительских долей
- юридический адрес;
- заявленные в уставе виды хозяйственной деятельности.

Наибольшую информационную ценность для службы конкурентной

разведки имеют о**тчеты** предприятий (организаций), т.к. в них содержится следующая **информация:**

- сведения о финансовом состоянии компании;
- итоги производственно-сбытовой деятельности за отчетный период;
- оценка стратегической перспективы предприятия (организации) на целевых рынках;
- информация о крупных поставщиках сырья, материалов, полуфабрикатов и т. п.;
- информация о крупных покупателях продукции предприятия (организации);
- сведения о руководстве предприятия (организации);
- сведения о системе принятия решений на предприятия (организации);
- данные о рисках, возникающих в процессе функционирования предприятия (организации) и т. д.

Отчетность открытых (публичных) акционерных обществ содержится на официальных сайтах хозяйствующих субъектов, на специализированных порталах раскрытия информации, в средствах массовой информации, на собрании акционеров. **Юридические лица других организационно-правовых форм** законодательно не обязаны составлять подобные отчеты, а также не обязаны публиковать баланс и отчет о прибылях и убытках в открытых источниках информации.

Распространенной практикой получения соответствующей документации является запрос её у самого предприятия (организации), интересующую службу конкурентной разведки, в ходе заключения, например, крупных контрактов или оформление доступа к системам хранения информации, например, к базе данных «Интегрум», самого полного на сегодняшний день электронного архива авторитетных источников информации о России.

Анализируя соответствующую документацию специалисты службы конкурентной разведки формируют заключение о состоянии дел отдельного предприятия (организации) с целью снижения рисков заключения контрактов с ненадежными подрядчиками или покупателями, а также рыночного позиционирования собственного предприятия (организации) на целевых рынках.

К официальным материалам относятся также р**аспоряжения, приказы и иная внутренняя документация** предприятий (организаций). Эти источники, чаще всего, имеют закрытый характер, что делает их недоступными для службы конкурентной разведки. Однако часть этих документов может добровольно предоставляться хозяйствующим субъектом в составе тендерной документации, размещаться на собственном сайте, публиковаться в многотиражных изданиях, что делает эти материалы открытыми. Размещенные же во внутренних базах данных предприятия (организации)

или на информационных стендах во внутренних помещениях исследуемого объекта материалы могут также стать доступными для службы конкурентной разведки.

Рекламные материалы и публикации, рассматриваемые службой конкурентной разведки в качестве источника информации - это статьи, объявления, пресс-релизы, рекламные модули, презентации, аудио - и видеозаписи и иные документы. Исследуемое предприятие (организация) может доводить информацию о себе и своих предложениях до целевой аудитории и широкой публики через различные каналы: наружная реклама, пресса, радио, телевидение, телефонные справочники, Интернет и т.п.

Упоминания предприятий (организаций) **и отзывы о них** являются важнейшим источником информации, т.к. хотя они и распространяются при помощи тех же каналов, что и рекламные материалы, но не от лица самих хозяйствующих субъектов, а от так называемых «третьих» лиц. Этот факт придает данному источнику информации большую объективность. Однако, используя эти материалы, специалисты службы конкурентной разведки должны иметь в виду, что в некоторых случаях подобные публикации могут быть инициированы самими хозяйствующими субъектами, например, при организации так называемой скрытой рекламы.

Прайс-листы (прейскуранты, тарифы и т.п.) являются документами, к структуре и информационному наполнению которых законодательством не предъявляется каких-либо требований, поэтому их форма и содержание существенно варьируются предприятиями (организациями). Наряду со счетами и коммерческими предложениями прайс-листы являются важным источником информации для изучения ценовой и ассортиментной (номенклатурной) политики партнёров и конкурентов, в предельной полноте, достоверности и актуальности которого заинтересованы, прежде всего, сами его авторы.

Объявления о появлении **вакансий** на предприятии (в организации) размещаются на разных носителях, и в первую очередь – на Интернет - ресурсах: корпоративных сайтах, ресурсах кадровых агентств, в виде контекстной и баннерной рекламы и т.п. Эти источники позволяют определить уровень заработной платы в анализируемом хозяйствующем субъекте, основные требования к персоналу, его организационную и управленческую структуры. Публикуемые предприятием (организацией) объявления о кадровых вакансиях позволяют специалистам службы конкурентной разведки сделать выводы о его потенциальном выходе на новые товарные рынки или о запуске на его производстве новых направлений бизнеса до появления в открытом доступе соответствующей официальной информации.

Но при работе с информацией из данного источника следует иметь в виду:

- зачастую в кадровых объявлениях размещается информация не обо всех имеющихся на предприятии (в организации) вакансиях, т.к. существует практика замещения «ключевых» вакансий из корпоративного

кадрового резерва или использования прямых способов подбора кандидатов;

- требования к кандидатам часто не соответствуют характеристикам, которыми будет обладать нанятый в итоге персонал: предварительно указанная квалификация кандидатов на замещение вакантных должностей может сознательно ужесточаться специалистами кадровой службы, а некоторые «очевидные» для работодателя ключевые навыки могут не упоминаться в объявлении о вакансии.

Резюме претендентов на вакансии на предприятии (в организации) могут публиковаться в средствах массовой информации, рассылаться по факсу и электронной почте, помещаться на персональных сайтах, блогах или в социальных сетях, пересылаться обычной почтой, доставляться лично. Их анализ позволяет службе конкурентной разведки хозяйствующего субъекта, осуществляющего подбор кадров, получать не только информацию о профессиональной биографии кандидата, но и некоторые данные о фирмах, в которых он работал раньше (например, наличие в штате этих фирм сотрудников определённой квалификации). Однако при работе с данными из резюме претендентов следует иметь в виду, что содержащаяся в них информация может быть неполной, недостоверной и формализованной.

Техническая документация, используемая службой конкурентной разведки предприятия (организации) для изучения продукции конкурентов при отсутствии доступа к образцам товаров – это соответствующие каталоги, чертежи, 3D-модели и т.п. Техническая документация может размещаться в открытом доступе, например, на сайте изучаемого хозяйствующего субъекта, а может предоставляться адресатом по соответствующему запросу.

Инвестиционные программы, программы закупок и перечни закупаемой продукции используются предприятиями (организациями) как для распространения информации о своей инвестиционной привлекательности, так и для снижения издержек на поиск информации о потенциальных поставщиках ресурсов для собственного производства. Как правило, эта информация размещается в свободном доступе, т.к. в её широком распространении заинтересован, прежде всего, сам хозяйствующий субъект, о чьих программах в данном случае идёт речь. Специалисты конкурентной разведки используют данную информацию для прогнозирования потенциальной емкости товарного рынка, стратегического планирования производственно-сбытовой деятельности собственного предприятия (организации) с учетом перспективного тренда развития целевых рынков.

В инвестиционных программах обычно содержится описание объектов инвестиций, указываются сроки реализации инвестиционного проекта и планируемые суммы капиталовложений. Инвестиционные программы,

разрабатываемые федеральными и региональными органами власти, включаются в текст законов о бюджете Российской Федерации и её субъектов. В этом случае названия объектов, заказчики, сроки выполнения и размер финансирования публикуются раньше, чем соответствующая конкурсная документация появляется на сайте www.zakupki.gov.ru, поэтому хозяйствующие субъекты, работающие с госзаказами, могут ей пользоваться для предварительного установления коммерческих отношений с лицами, принимающими решения со стороны заказчика.

Программы закупок обычно содержат перечень и объемы планируемых к приобретению в указанный период товаров для текущей деятельности предприятия (организации), а **перечень закупаемой продукции** содержит только наименование приобретаемых товаров без указания объемов. Неотъемлемой частью названных документов являются так называемые у**словия сотрудничества:** перечень требований к контрагентам, которые необходимо соблюсти для начала работы с тем или иным хозяйствующим субъектом. В некоторых случаях эти условия могут быть закрытой информацией, в других же случаях эта информация публикуется в Интернете, средствах массовой информации или рассылается по каналам связи предприятиям (организациям), заинтересованным в соответствующем сотрудничестве.

Референс-листы – это перечни реализованных проектов или укомплектованных объектов, в работе над которыми приняла участие то или иное предприятие (организация). Данные документы или публикуются в открытом доступе, или рассылаются заинтересованным лицам по соответствующему запросу. Наличие референс-листов может быть обязательным условием для участия хозяйствующего субъекта в тендере. Однако при работе с референс-листами специалисты службы конкурентной разведки должны учитывать, что в них могут не упоминаться незначительные проекты, в реализации которых принимало участие анализируемое предприятие (организация), а также проекты, вызвавшие нарекания заказчика.

Тендерная документация является важным источником информации о контрагентах анализируемого предприятия (организации), его реализованных проектах и планах. Тендеры, конкурентные торги, запросы котировок могут проводить организации любых форм собственности. Порядок участия в данных мероприятиях регулируется внутренними документами таких хозяйствующих субъектов. Если речь идет о торгах для государственных и муниципальных нужд, данные правоотношения регулируются Законом от 21 июля 2005 г. № 94-ФЗ «О размещении заказов на поставки товаров, выполнение работ, оказание услуг для государственных и муниципальных нужд». Официальным сайтом для публикации информации о размещении государственных заказов является сайт www.zakupki.gov.ru. Доступ к информации, размещенной на этом сайте, осуществляется бесплатно. На сайте организована система поиска кон-

трактов, благодаря которой специалист конкурентной разведки может определить круг заказчиков и подрядчиков по государственным и муниципальным заказам с перечнем соответствующих работ (услуг), а также выявить предприятия (организации), которые не выполняют взятые на себя обязательства по данным контрактам.

Отчеты по результатам рыночных исследований – источник информации, используемый специалистами конкурентной разведки для изучения внешней среды того или иного предприятия (организации). Результаты исследований рынка обычно оформляются в виде отчетов консалтинговых организаций, некоторые из которых можно приобрести на коммерческой основе. Отчеты о результатах маркетинговых исследований публикуются также органами власти (например, Государственной антимонопольной службой) и некоммерческими организациями (например, гильдией маркетологов).

3.3. Вещи как источники информации

Вещи (материальные объекты), рассматриваемые специалистами конкурентной разведки в качестве источника информации, представлены на рис. 15.

Рис. 15. Вещи, рассматриваемые специалистами конкурентной разведки в качестве источника информации

Общая характеристика вещей как источников информации представлена ниже.

Образец (эталон, товарный прототип) **продукции** - это образец изделия, изготавливаемый промышленным способом в одном или нескольких (партией) экземплярах до внедрения в серийное производство с целью опытной проверки и контроля конструктивно-технических и потребительских качеств, предусмотренных техническим заданием на его проектирование и проектом. Как правило, изготовление образца продукции или его партии – обязательный этап разработки новых (модернизированных) товаров.

Анализируя образцы товаров, специалисты службы конкурентной разведки могут сделать выводы о технологии их производства, используемых материалах и применяемых технологиях. Данная информация позволяет определить конкурентные преимущества продукции собственного предприятия (организации), понять причины различия в цене внешне аналогичных изделий, продаваемых разными поставщиками. С образцами продукции для их последующего изучения сотрудники службы конкурентной разведки могут ознакомиться на выставках, семинарах, в торговых залах изготовителя (перепродавца). Также возможен вариант покупки образцов под видом клиента.

Муляж продукции – это собой слепок или модель товара (изделия) в натуральную величину. Муляжи используются в качестве выставочных образцов в том случае, когда настоящие образцы продукции демонстрировать по каким-то причинам невозможно или нецелесообразно. Муляжи воспроизводят только внешний вид изделий, поэтому фактически сотрудники конкурентной разведки предприятия (организации) могут использовать их лишь для изучения габаритов изделий и товарного дизайна.

Макет продукции – это модель объекта в уменьшенном (увеличенном) масштабе или в натуральную величину, лишённая, как правило, функциональности представляемого товара. В макете могут отсутствовать или быть изображены условно детали, не влияющие на ход требуемого для демонстрации процесса. Макеты изготавливаются для представления объекта на выставках или при его публичной демонстрации. При изучении макетов специалист конкурентной разведки получает лишь некую общую информацию об интересующем его изделии, включая область применения, принцип его работы и внешний вид.

Выставочное оборудование – это различные стенды, витрины, стойки, на которых размещается товар или иные предметы выставки.

Торговое оборудование – это оборудование, предназначенное для предприятий торговли, используемое для выкладки, хранения и продажи товаров. Характеристика групп торгового оборудования представлена на рис. 16.

Офисная техника — техническое оборудование офиса, облегчающее и ускоряющее бумажное делопроизводство, а также административно-управленческую деятельность на предприятии (в организации).

Складская техника предназначена для механизации (автоматизации) работы на открытых и закрытых складах товарно-материальных ценностей товаропроизводителей и логистических организаций. Требования, предъявляемые к складской технике: маневренность, мобильность, компактность, экологичность (отсутствие вредных выбросов при работе).

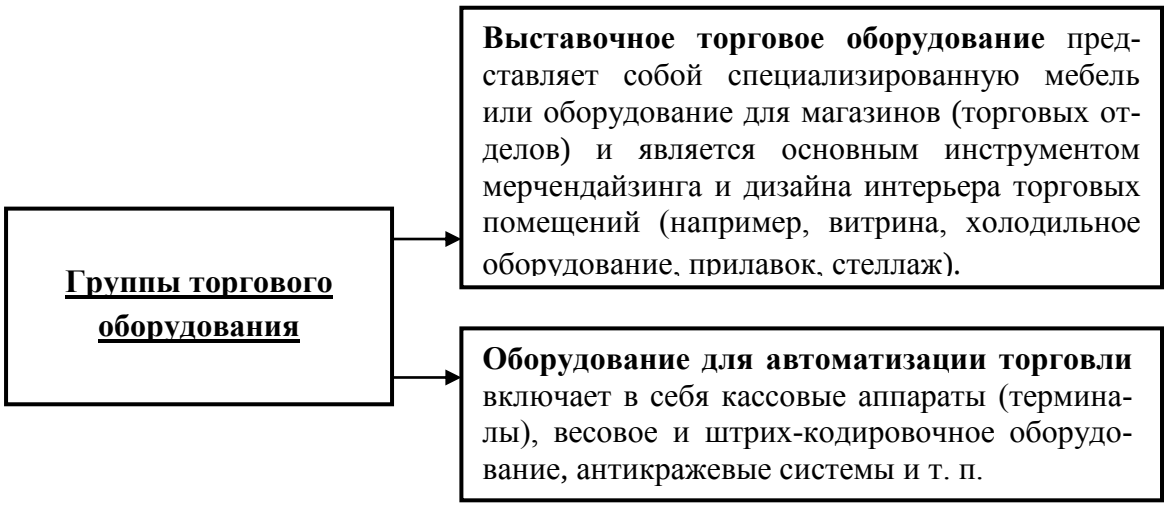

Рис. 16. Характеристика групп торгового оборудования

Виды складской техники подразделяется на виды:

- собственно складская техника:
  - упаковочная техника;
  - техника создания транспортных единиц;
  - техника транспортирования;
  - техника складирования;
  - техника комплектации (комиссионирования);
  - техника владения;
  - монтажная техника;
  - погрузочно-разгрузочная техника;
  - информационная техника и техника управления;
- техника хранения и передачи информации;
- техника управления.

Выставочное и торговое оборудование, офисная и складская техника дают специалисту конкурентной разведки информацию о политике продвижения того или иного предприятия (организации), технологиях его продаж и уровне сервиса.

3.4.Выставки (конференции) в работе конкурентной разведки

Выставка – это собрание каких-нибудь предметов или живых существ (животных), расположенных где-либо для обозрения, а также место такого обозрения. Как правило, выставка - это публичное представление достижений в области экономики, науки, техники, культуры, искусства и других областях общественной жизни. Понятие «выставка» может обозначать как само мероприятие, так и место его проведения.

Конференция – это собрание, совещание групп лиц (отдельных лиц), которое организовано для обсуждения определённой проблемы или ряда вопросов продолжительностью, как правило, более одного дня.

Выставки и конференции активно используются как для сбора, так и

для предоставления информационных благ.

Информационные блага, предоставляемые выставками (конференциями) их участникам:

- возможность знакомства с образцами продукции предприятий (организаций);
- возможность получения личной консультации специалиста по интересующим вопросам;
- возможность получения различных информационных материалов на материальных носителях;
- возможность установления личных контактов с сотрудниками предприятий (организаций), присутствующими на мероприятии (руководящим, коммерческим и техническим персоналом хозяйствующих субъектов);
- возможность получения эксклюзивной неформальной (непубликуемой) информации в ходе личного общения с присутствующими на мероприятии специалистами;
- возможность сбора информации для сравнительного анализа продукции, коммуникаций, технологии и т.п. нескольких конкурирующих предприятий (организаций), участвующих в мероприятии.

Специалисты конкурентной разведки разделяют выставки (конференции) на **профильные** (специализированные) и **непрофильные** (общего характера).

Ниже рассмотрена работа службы конкурентной разведки предприятия (организации) на **профильных** выставках (конференциях), предоставляющих возможность получения конфиденциальной информации коммерческого или научно-технического характера не только от товаропроизводителей, но и от так называемых смежников, поставщиков, банков, инвесторов и т.д. Особая ценность информации, полученной на подобных мероприятиях, заключается в получении её из первоисточника.

Формы работы специалиста конкурентной разведки на выставке (конференции):

- в качестве участника;
- в качестве посетителя (зрителя);
- в качестве удалённого аналитика выставочных материалов (материалов конференции), т.е., без личного присутствия на мероприятии.

По времени работа специалистов службы конкурентной разведки подразделяется на периоды:

- подготовительный период;
- время работы на выставке (конференции);
- время аналитической работы по окончании выставки (конференции).

Этапы подготовительной работы службы конкурентной разведки для эффективного участия в работе выставки (конференции) представлены на рис. 17.

Рис. 17. Этапы подготовительной работы службы конкурентной разведки предприятия (организации) перед участием её специалистов в работе выставки (конференции)

Общая характеристика этапов подготовительной работы службы конкурентной разведки предприятия (организации) перед участием её специалистов в работе выставки (конференции) представлена ниже.

Первый этап: получение информации о запланированном мероприятии по следующим **каналам**:

- информационные рассылки организаторов выставки (конференции) по почте и каналам Интернет;
- информационные рассылки администрации выставочных комплексов выставки (конференции) по почте и каналам Интернет;
- редакционные и рекламные материалы печатных и электронных средств массовой информации;
- официальные сайты хозяйствующих субъектов.

Второй этап: определение привлекательности выставки (конференции) для службы конкурентной разведки предприятия (организации) и **принятие решения** о необходимости участия в ней (в нём).

Решение специалисты службы конкурентной разведки принимаются в зависимости от того, какие ответы будут получены **на вопросы**:

- входит ли в программу выставки (конференции) рассмотрение проблем, входящих в круг бизнес – интересов предприятия (организации);
- насколько репрезентативным с точки зрения предприятия (организации) является заявленный в программе состав заявленных к участию в выставке (конференции) экспертов, специалистов, хозяйствующих субъектов (включая конкурентов);
- каков предполагаемый уровень заявленного контингента участников выставки (конференции) и каковы заявленные в программе цели её (его) проведения.

Если по результатам информационного анализа принимается решение

об участи предприятия (организации) в работе выставки (конференции), служба конкурентной разведки разрабатывает **характеристики** специалистов, которые непосредственно будут направлены на соответствующее мероприятие для участия в нем в том или ином виде:

- количество специалистов службы конкурентной разведки и других административно-производственных подразделений предприятия (организации), привлекаемых к подготовительной работе перед участием в выставке (конференции), квалификационные требования, предъявляемые к соответствующим сотрудникам;
- количество специалистов службы конкурентной разведки и других административно-производственных подразделений предприятия (организации), направляемых непосредственно на выставку (конференцию), для участия в ней (нем), квалификационные требования, предъявляемые к соответствующим сотрудникам;
- количество специалистов службы конкурентной разведки, других административно-производственных подразделений предприятия (организации) и сторонних экспертов, привлекаемых к аналитической работе с материалами, собранными в ходе участия предприятия (организации) в выставке (конференции), квалификационные требования, предъявляемые к соответствующим сотрудникам.

Третий этап (не обязательный)**: формирование** группы участников (так называемой «разведгруппы») производится в случае, если даже после тщательной подготовки к участию в выставке (конференции) одному специалисту в ходе проведения мероприятия будет сложно собрать весь объем необходимой и доступной информации.

Участие службы конкурентной разведки в работе выставки (конференции) должно быть конфиденциальным, в том числе – для сотрудников самого предприятия (организации). Для её обеспечения с одной стороны, и достижения поставленных целей и задач – с другой, «разведгруппу» должен возглавлять один из ведущих специалистов службы конкурентной разведки, однако ни в коем случае не её начальник.

Кроме сотрудников службы конкурентной разведки в состав «разведгруппы», при необходимости, на выставку (конференцию) направляются профильные сотрудники предприятия (организации), которые могут присутствовать на мероприятии и как официальная делегация, и как эксперты.

Основными требованиями к сотрудникам – членам «разведгруппы» является их компетентность:

- в сфере деятельности собственного предприятия (организации);
- в сфере деятельности ведущих конкурентов;
- в области стратегических целей собственного предприятия (организации);
- в области развития товарного и территориального рынка;
- в вопросах технологии получения информации из первоисточника, в

качестве которого в опосредствованном виде выступает выставка (конференция).

Четвертый этап: разработка «легенды», под которой члены «разведгруппы» будут присутствовать на выставке (конференции), и изготовление соответствующих документов прикрытия.

Появление данного этапа подготовительной работы обусловлено необходимостью соблюдения режима секретности (конфиденциальности) при любом выходе сотрудников службы конкурентной разведки предприятия (организации) в открытую рыночную среду с целью проведения полевых исследований.

Следовательно, при реализации мероприятий конкурентной разведки на выставке (конференции) специалистам нужна надежная, проработанная конспирация, поскольку их деятельность ни при каких условиях не должна ассоциироваться с предприятием (организацией), в которой они работают. Поэтому при подготовке сотрудников «разведгруппы» к работе на выставке (конференции) им прописывается соответствующая «легенда» и выдаются документы прикрытия, использование которых удовлетворяло бы названным выше условиям.

Варианты «легенд» для членов «разведгруппы»:

- представитель прессы, в т.ч. корпоративной;
- эксперт в определенной профессиональной отрасли товарного производства, коммерческого сервиса или прикладной (фундаментальной) науки;
- социолог, осуществляющий опрос участников в статистических или правовых целях;
- представитель коммерческой инфраструктуры (поставщиков, логистических, посреднических, девелоперских компаний, банков, фондов и т.п.);
- специальная легенда (например, представитель правозащитной или некоммерческой организации, политической партии и т.п.).

Виды документов прикрытия:

- визитные карточки;
- бейджи;
- бланки, анкеты, листовки и прочий «раздаточный» материал;
- специальный сайт в интернете с соответствующей контактной информацией;
- иные документы, отвечающие специфике предприятия (организации).

Особое внимание следует уделять подготовке информации «обратной связи» на случай проверки данных легенд и документов прикрытия членов «разведгруппы» непосредственно во время проведения выставки (конференции). Вся используемая специалистами в работе на мероприятии информация должна быть либо реальной, либо непроверяемой по причинам, не вызывающим подозрений у оппонента (например, сезонный отъезд интересующего оппонента сотрудника в научную экспедицию).

Все предъявляемые членами «разведгруппы» непосредственно во время проведения выставки (конференции) её участникам документы прикрытия (например, визитные карточки) должны отвечать **требованиям:**

- содержать минимальное количество объективной информации;
- не привлекать к себе излишнего внимания ни своей простотой, ни излишней красочностью.

Пятый этап: позиционная рекогносцировка. В ходе неё разрабатывается конкретный перечень источников информации на выставке (конференции) с распределением этих объектов между сотрудниками – участниками «разведгруппы» для получения информации в соответствии со спецификой квалификации экспертов-разведчиков. Если для получения всего объема интересующей «разведгруппу» информации необходимо несколько подходов к одному источнику информации разными экспертами, определяется последовательность и время подхода для каждого члена группы, работающего с данным объектом.

В ходе рекогносцировки предстоящее мероприятие анализируется по позициям, перечисленным ниже:

- участие в мероприятии объектов получения информации, включая конкурентов;
- участие в мероприятии экспертов, специалистов, топ-менеджеров сторонних хозяйствующих субъектов по интересующим «разведгруппу» темам;
- время и место проведения конкретных событий выставки (конференции): докладов, презентаций, круглых столов и т.п.

По результатам подготовительного периода служба конкурентной разведки предприятия (организации) разрабатывает план работы «разведгруппы» на выставке (конференции), в котором должны быть **определены**:

- порядок и способы связи между сотрудниками во время работы на выставке (конференции);
- место и время промежуточных сборов сотрудников для обмена информацией во время работы на выставке (конференции);
- место и время сбора сотрудников по завершению мероприятия.

Предварительная подготовка к выставке (конференции) заканчивается в момент прибытия делегации предприятия (организации), включая «разведгруппу», на место проведения мероприятия. В данном случае под «местом проведения» имеется в виду не только непосредственно выставочный зал или академическая аудитория, но и соответствующий населённый пункт, так как часть интересующей службу конкурентной разведки информации можно получить в гостиницах, где проживают участники выставки (конференции).

Алгоритм работы специалистов службы конкурентной разведки на выставке (конференции) представлен ниже.

В первый день работы выставки (конференции) рабочей группой

службы конкурентной разведки осуществляется первичный осмотр экспозиции для корректировки плана проведения полевых мероприятий по сбору информации, а также – её первоначальный анализ. В ходе анализа узкие специалисты дают профессиональную оценку представленных экспонатов, в том числе – новых товаров или впервые появляющихся на рынке (в информационном пространстве) хозяйствующих субъектов (включая малых).

Перечень задач, решаемых службой конкурентной разведки в последующие дни проведения выставки (конференции), представлены на рис. 18.

Рис. 18. Задачи, решаемые членами «разведгруппы» на выставке (конференции)

Эффективность работы группы конкурентной разведки на выставке (на конференции) определяется объемом и ценностью собранной за это время информации. **Пути** повышения эффективности названной работы:

- посещение членами «разведгруппы» запланированных на выставке (конференции) мероприятий в полном объеме;
- проведение членами «разведгруппы» бесед со специалистами, присутствующими на выставке (конференции), в соответствии с утвержденным во время подготовительного периода планом;
- максимальное внимание членов «разведгруппы» к содержанию

представленных на выставке (конференции) докладов и сообщений, видео и аудио презентаций конкурентов и других участников рынка;

- проведение членами «разведгруппы» собственных полевых исследований во время проведения выставки (конференции) под видом легенды – прикрытия, например, социальных опросов среди участников и посетителей мероприятия.

Все полученные членами «разведгруппы» за время работы выставки (конференции) данные передаются эксперту из числа сотрудников службы конкурентной разведки, для их первичной систематизации, анализа и определения объёма дополнительной информации, которую необходимо получить до окончания мероприятия.

К числу **приоритетных источников информации** для членов «разведгруппы» на выставке (конференции) относятся:

- стенды (доклады) конкурирующих с предприятием (организацией) хозяйствующих субъектов;
- прямые контакты членов «разведгруппы» со сторонними экспертами (специалистами).

Характеристика названных источников информации представлена ниже.

Стенды (доклады) являются тем источником информации, которые любому участнику проводимого мероприятия позволяют получить достоверную информацию о представленном хозяйствующем субъекте, о его продукции и его достижениях по вопросам, являющимся профильными на проводимой выставке (конференции). Статус участника позволяет членам «разведгруппы» задавать любые, даже излишне непрофессиональные («наивные») вопросы, т.к. участник не обязан быть экспертом в представленной на стенде (обсуждаемой в докладе) области. Следовательно, «разведчик», задавая свои вопросы может рассчитывать на получение конкретизирующих уже имеющуюся у него информацию данных. Кроме того, изучение презентационного стенда хозяйствующего субъекта одновременно с проведением соответствующих презентаций или переговоров с первыми лицами предприятий (организаций)позволяет сделать выводы о перспективных планах конкурентов (партнёров).

Выставка (конференция) – это место обмена мнениями, информацией между интересующими службу конкурентной разведки объектами (персоналиями или компаниями), где люди подсознательно готовы к общению. Среди участников находятся технические специалисты, обладающие знаниями в области коммерции или технологии производства, которые при других обстоятельствах могут рассматриваться как коммерческая тайна. Следовательно, члены «разведгруппы» обязаны обладать навыками не только по установлению личностных контактов, но и умением «разговорить» собеседника. К **основным методам по установлению контакта** с интересующим экспертом (специалистом) относятся:

- обладание навыками активного слушателя, т.е. умение грамотно применять в разговоре паузы, уточнения, повторы, замечания, сообщения о восприятии и т.п.;
- «оплата» полученной информации путём предоставления оппоненту ответной информации;
- выведение собеседника на доказательство собственной позиции, например, путём аргументированных доказательств мнения, не совпадающего с мнением собеседника.

Если выработанный на предварительном этапе план работы «разведгруппы» на выставке (конференции) требует осуществления многочисленных подходов к источнику информации, на практике могут осуществляться варианты работы с этим источником, представленные на рис. 19.

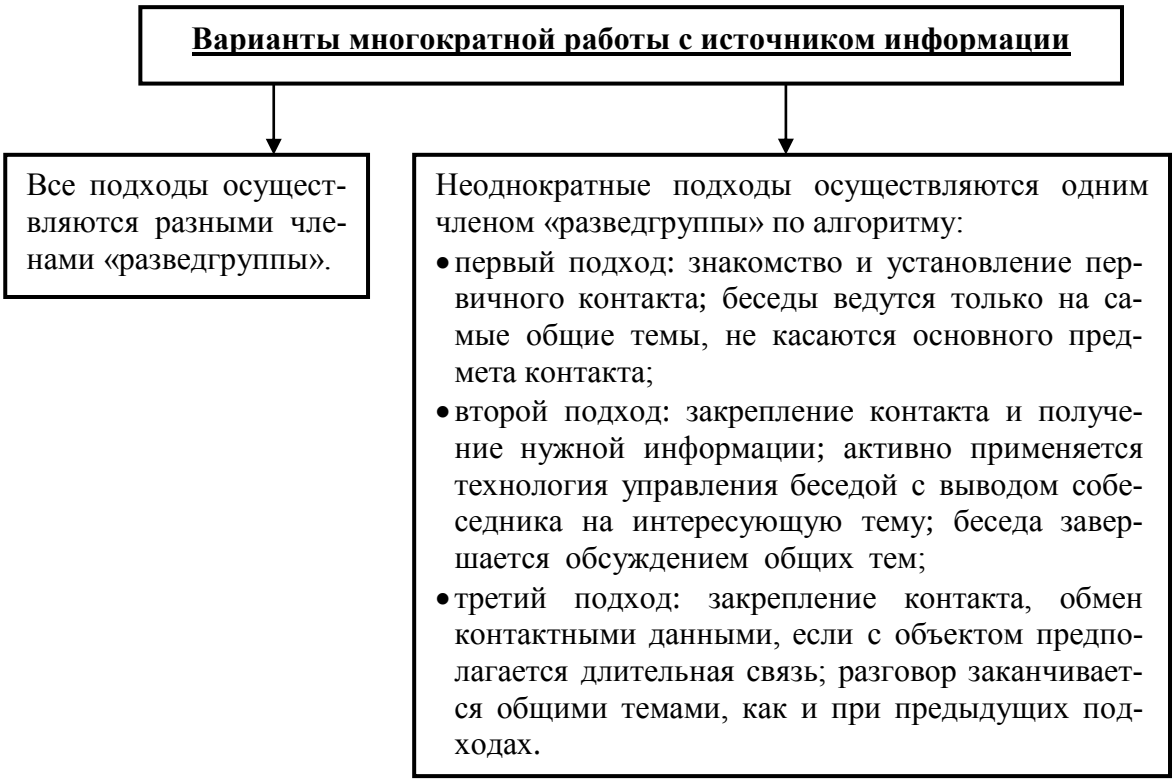

Рис. 19. Характеристика вариантов многократной работы с источником информации членами «разведгруппы» на выставке (конференции)

Дополнительные источники информации на выставках (конференциях):

- общедоступный раздаточный материал (буклеты, презентации и т.д.);
- специализированная литература, продаваемая в ходе проведения мероприятия специализированными продавцами.

Основные ошибки, допускаемые сотрудниками службы конкурентной разведки предприятия (организации) в статусе участника выставки (конференции):

- смена «легенды» членов «разведгруппы» во время проведения мероприятия;

- провокация ситуации, при которой происходит идентификация настоящей личности члена «разведгруппы).

3.5. Использование материалов СМИ в конкурентной разведке

В правовых документах Российской Федерации под средством массовой информации (СМИ) понимаются периодическое печатное издание, сетевое издание, телеканал, радиоканал, телепрограмма, радиопрограмма, видеопрограмма, кинохроникальная программа, любая иная форма периодического распространения массовой информации под постоянным наименованием (названием).

Перечень **наиболее распространенных** средств массовой информации представлен на рис. 20.

Рис. 20. Перечень наиболее распространенных средств массовой информации на территории РФ

В соответствии со способом распространения по территории страны (среди представителей целевой аудитории) массовой информации подразделяются на печатные и электронные.

Причины современного снижения роли печатных СМИ как источников информации:

- современные газеты и журналы имеют свои представительства в Интернете, включая архив выпусков;
- все большее распространение получают сетевые издания, не имеющие бумажных версий.

Виды информационно-аналитической работы со средствами массовой информации сотрудниками службы конкурентной разведки предприятия (организации):

- текущий мониторинг: специалист конкурентной разведки отслеживает новые материалы по мере их публикации;
- ретроспективный мониторинг: специалист конкурентной разведки работает с архивными материалами средств массовой информации.

Текущий мониторинг позволяет предприятиям (организациям) вовремя отслеживать наметившиеся или уже произошедшие рыночные, экономические, политические, социальные и т.п. тенденции или спрогнозировать возможные события. К числу последних относятся готовящиеся законодательные инициативы, которые могут повлиять на бизнес; появление новых рыночных игроков; появление новой продукции конкурентов; перестановки во властных структурах, в руководстве фирм конкурентов, партнеров, контрагентов и т.д.

Архивная работа позволяет предприятиям (организациям) в ходе ретроспективного мониторинга материалов СМИ выстраивать событийно - временные цепочки, посредством которых аналитик может выявить определенные взаимосвязи, что является основой для моделирования службой конкурентной разведки долгосрочной стратегии конкурента и его потенциальных действий в рамках этой стратегии. Кроме того, анализ архивных материалов является основой корректировки психологического профиля или репутационного имиджа отдельных сотрудников, способных активно влиять на деятельность соответствующих хозяйствующих субъектов.

В настоящее время техническая работа, проводимая средствами массовой информации с собственными информационными продуктами, позволяет службе конкурентной разведки предприятия (организации) автоматизировать информационно-аналитическую работу с материалами СМИ за счет:

- оцифровки текущих и архивных материалов;
- структурирования архивных материалов;
- индексации архивных материалов.

Индексация архивных материалов производится с целью создания объективных условий для быстрого поиска необходимой информации по ключевым словам, именам или названиям организаций.

Структурирование архивных материалов обеспечивает оптимальную выдачу сгруппированных в заданном исследователем порядке найденных материалов.

Радио и телевидение увеличивают своё значение в качестве источников информации для службы конкурентной разведки, т.к. на их сайтах сегодня размещаются записи всех или избранных передач, в том числе – текстовые расшифровки соответствующего аудиоряда. Однако мониторинг телевизионных и радиопрограмм является более сложным, чем работа с материалами печатных СМИ, в том числе и с точки зрения технического оснащения этой работы.

Сегодня на информационном рынке работает большое количество специализированных организаций, предлагающих доступ к электронным архивам средств массовой информации, с ежедневным поступлением новых документов. Это в определенной степени позволяет службе конкурентной разведки предприятия (организации) решать некоторые оперативные задачи текущего мониторинга материалов СМИ. Добиться полного удовлетво-

рения информационных потребностей бизнеса исключительно с помощью ресурсов централизованных хранилищ публикаций СМИ невозможно, т.к. в них размещаются не все публикации. В частности, как правило, в них отсутствуют материалы малотиражных или районных (местных) изданий.

По направленности статьи в СМИ можно разделить на:

- обзорные;
- дискредитирующие;
- рекламные;
- разглашающие коммерческую тайну.

Использование открытых источников в виде средств массовой информации позволяет в значительно снижать репутационные и имиджевые риски для предприятия (организации) при его работе на целевых рынках.

Классификация информации, получаемой из материалов СМИ, представлена на рис. 21.

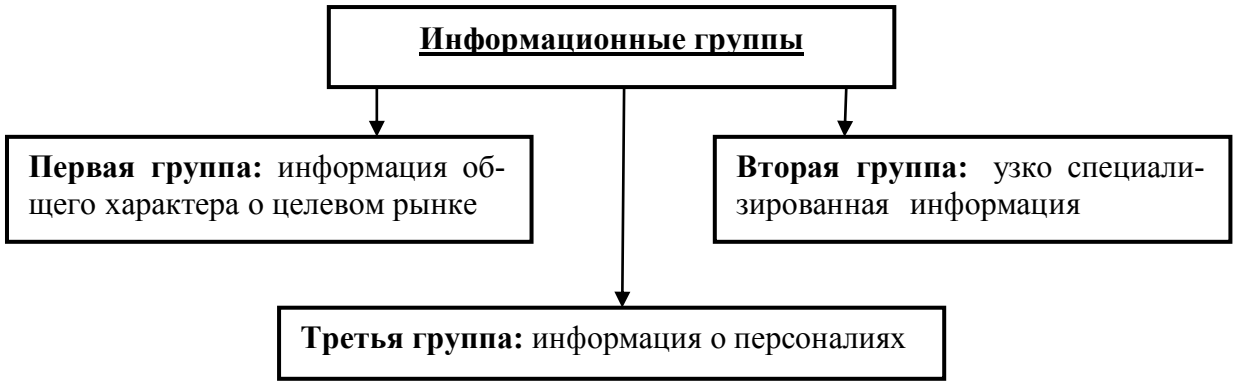

Рис.21. Классификация информации, получаемой службой конкурентной разведки из материалов СМИ

Ответственный исполнитель службы конкурентной разведки предприятия на постоянной основе проводит собственное (корпоративное) архивирование материалов СМИ с целью подготовки их для последующей камеральной работы. Процесс архивирования включает в себя обработку публикаций, их сортировку в соответствии с разработанным корпоративным классификатором и хранение. Для наиболее удобного последующего использования все данные заносятся в единую базу (интегрированный банк данных).

Правила организации информационной работы с прессой:

- правильный подбор источников информации;
- обработка источников информации с использованием принципа «ключевых слов»;
- грамотная организация сортировки, классификации и хранения отобранной информации.

Ключевые слова – особо важные, общепонятные, ёмкие и показательные для отдельно взятой проблемы (темы) слова в тексте, набор которых может

дать высокоуровневое описание содержания анализируемого текста для читателя, обеспечив компактное представление и хранение его смысла в памяти.

К набору слов из текста применим термин «ключевые слова», если эти слова имеют следующую **характеристику:**

- они являются наиболее употребительными в частотном смысле наименованиями и обозначают признак предмета, состояние или действие;
- они представлены значимой лексикой, достаточно обобщены, т.е. обладают средней степенью абстракции, стилистически нейтральны, не носят оценочного характера;
- они связаны друг с другом сетью семантических (тематических) связей и пересечения значений;
- они составляют более половины от количества слов, составляющих так называемое ядро тематического компонента, а их минимальный набор приближается к инварианту, т.е.сути содержания при их логическом упорядочивании;
- их количество равно 5 – 15 или 8 – 10 словам, что соответствует объему оперативной памяти человека;
- их набор определяет законченную в смысловом отношении часть текста.

Алгоритм извлечения ключевых слов из текста представлен на рис. 22:

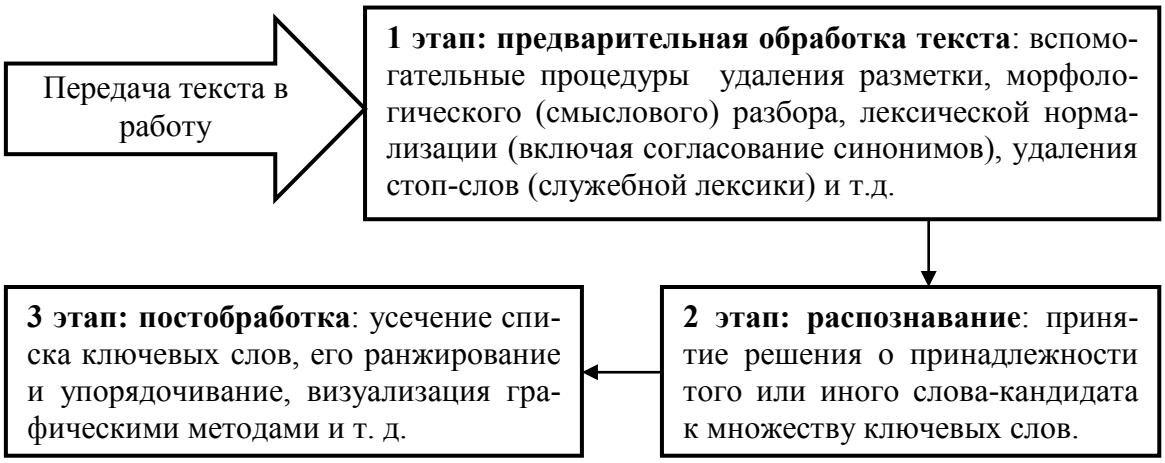

Рис. 22. Алгоритм извлечения ключевых слов из текста

Аналитической работе службы конкурентной разведки предприятия (организации) предшествуют следующие **подготовительные процедуры**:

- анализ нескольких выпусков (номеров) периодических изданий СМИ за определенный период времени (например, за неделю, месяц, год);
- формирование полного списка опубликованных в анализируемых выпусках СМИ статей;
- выбор набора изданий, наиболее полно удовлетворяющих информационные потребности предприятия (организации) по определенным информационным направлениям;

➢ периодическая актуализация произведенной выборки СМИ.

Этапы аналитической работы с прессой в подразделениях службы конкурентной разведки предприятия (организации):

1 этап – формулировка цели сбора (подбора) информации;

2 этап – определение информационных потребностей заказчиков информации;

3 этап – подбор источников информации.

Виды информации, получаемые службой конкурентной разведки в ходе аналитической работы над публикациями в СМИ:

➢ базовая информация;

➢ текущая информация (о фактах и событиях);

➢ субъективно-оценочная информация.

Полученные в ходе содержательного анализа массивы первично систематизированной и актуализированной информации подвергаются контент-анализу, результаты которого являются, как правило, итогом работы службы конкурентной разведки с материалами средств массовой информации.

Контент-анализ – техника аналитической работы с массивами текстов на основе выделения в тексте некоторых ключевых понятий или смысловых единиц и их дальнейшего сопоставления.

Необходимым условием применения метода контент-анализа является наличие материального носителя информации. Во всех случаях, когда существует или может быть создан такой носитель, допустимо использование метода контент-анализа.

Характеристика метода «Контент-анализ»:

➢ это метод качественно-количественного анализа содержания документов с целью выявления или измерения различных фактов и тенденций, отраженных в этих документах;

➢ это формализованный метод изучения текстовой и графической информации, заключающийся в переводе изучаемой информации в количественные показатели и её последующей статистической обработке;

➢ этот метод не отменяет необходимости обычного (т.е. содержательного) анализа документов, а дополняет его, сочетание двух методов углубляет понимание смысла любого текста.

Контент-анализ позволяет обнаружить в документе информационные связи, ускользающие от внимания исследователя при его традиционном изучении, но имеющие важный смысл в контексте изучаемой службой конкурентной разведки предприятия (организации) проблемы.

Принципиальным отличием метода контент-анализа от иных методов анализа текстовых документов является его явно выраженная строгость, формализованность и систематизированность. Метод нацелен на выработку количественного описания смыслового и символического со-

держания документа, на фиксацию его объективных признаков и подсчет последних.

Объектом контент-анализа может быть содержание различных печатных изданий, радио- и телепередач, кинофильмов, рекламных сообщений, документов, публичных выступлений, материалов анкет.

Началу работы по проведению контент-анализа **предшествуют:**

- формулировка темы, задач и гипотезы исследования;
- определение категорий анализа.

Категории контент-анализа – это наиболее общие, ключевые понятия, соответствующие исследовательским задачам.

Требования, предъявляемые к категориям контент-анализа:

- уместность: соответствие решению исследовательских задач;
- исчерпываемость: достаточно полное отражение смысла основных понятий исследования;
- взаимоисключаемость: одно и то же содержание не должно входить в различные категории контент-анализа в одинаковом объеме;
- надежность: неспособность вызывать разногласия между исследователями по поводу того, что следует относить к той или иной категории контент-анализа в процессе исследования документа.

Обязательные исследовательские инструменты, используемые при проведении контент-анализа, представлены на рис. 23.

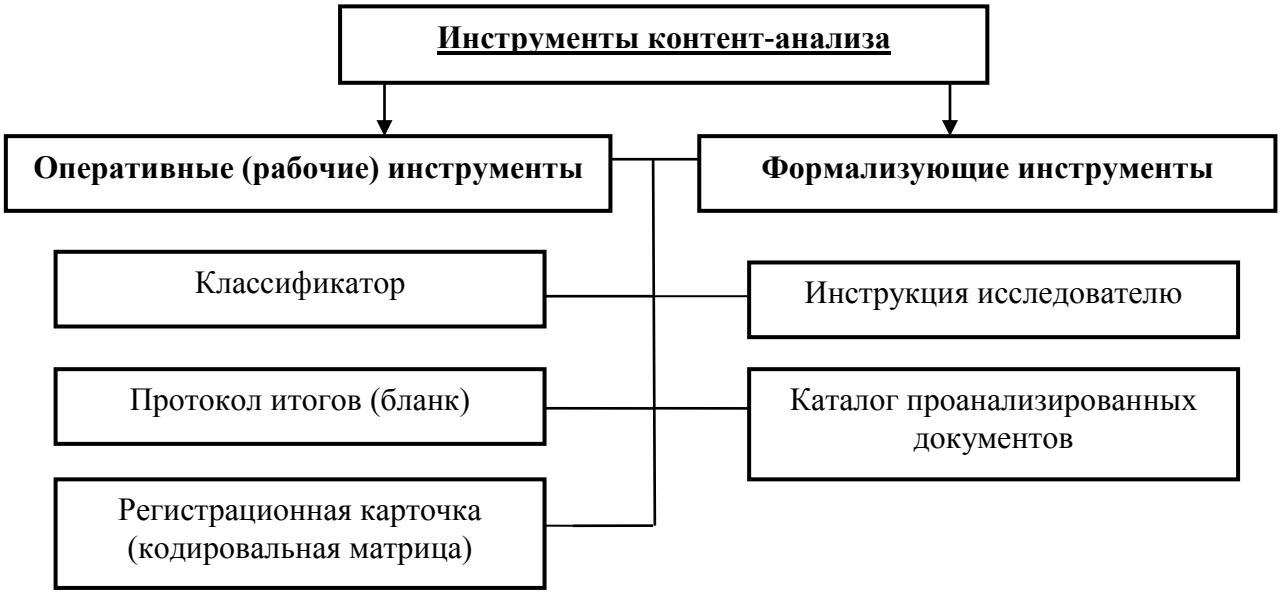

Рис. 23. Обязательные исследовательские инструменты, используемые при проведении контент-анализа

Разработка обязательных исследовательских инструментов осуществляется до начала проведения контент-анализа (предварительно). **Характеристика** исследовательского инструментария приводится ниже.

Классификатором контент-анализа называется общая таблица, в которую сведены все категории (и подкатегории) анализа, а также единицы анализа. Цель создания классификатора – четкая фиксация того, в каких единицах выражается каждая категория, используемая в исследовании. Аналогом классификатора является маркетинговая анкета, где категории анализа играют роль вопросов, а единицы анализа – роль ответов. Классификатор является основным методическим документом контент-анализа, определяющим содержание всех прочих инструментов этого метода.

Протокол (бланк) контент-анализа содержит:

- сведения об анализируемом текстовом документе (его авторе, времени разработки или создания, объеме анализируемого текста и т.п.);
- итоги анализа текстового документа (количество случаев употребления в документе определенных единиц анализа и следующие отсюда выводы относительно категорий анализа).

Протоколы обычно заполняются в **закодированном виде**, который позволяет наиболее удобно и компактно представит информацию об анализируемом документе. Цель кодирования – упрощение процедуры сопоставления друг с другом итогов анализа разных документов.

Регистрационная карточка представляет собой кодировальную матрицу, в которой отмечается количество единиц счета, характеризующее единицы анализа. Протокол контент-анализа каждого анализируемого документа заполняется на основе подсчета данных всех регистрационных карточек, относящихся к этому документу

Этапы проведения контент-анализа представлены на рис. 24.

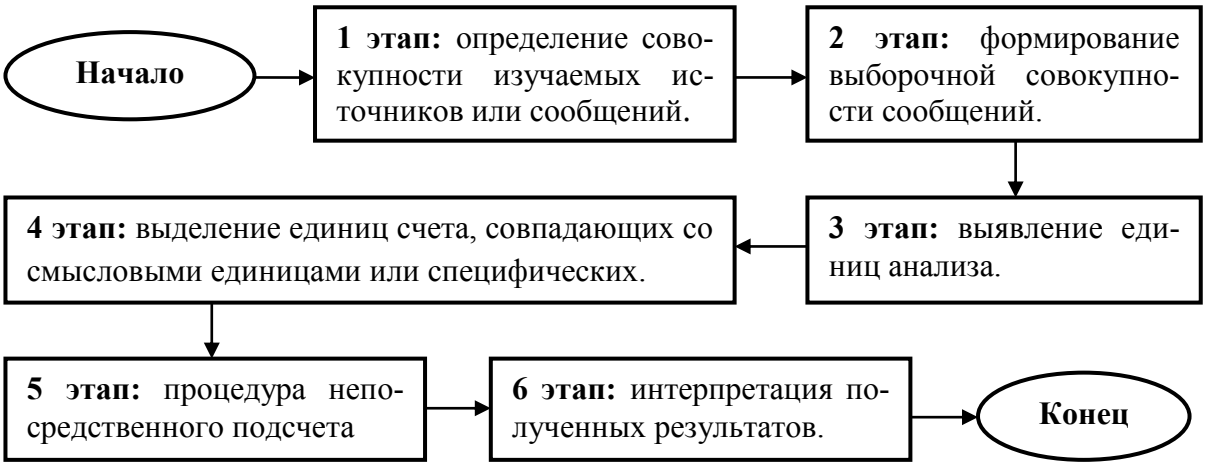

Рис. 24. Этапы проведения контент-анализа (общая схема)

Характеристика этапов проведения контент-анализа представлена ниже.

Первый этап: определение совокупности изучаемых источников или сообщений. Работа проводится с помощью набора заданных критериев, которым должно отвечать каждое сообщение:

- определенный тип источника (пресса, телевидение, радио, рекламные или пропагандистские материалы)
- определенный тип сообщений (статьи, заметки, плакаты);
- заданные стороны, участвующие в процессе коммуникации, а именно отправитель и получатель;
- сопоставимый размер сообщений (минимальный объем текста или физическая длина и ширина напечатанного материала);
- частота появления сообщений;
- способ распространения сообщений;
- место распространения сообщений;
- время появления сообщений.

Перечисленные выше критерии являются наиболее часто употребляемыми в практике проведения контент-анализа службами конкурентной разведки предприятия (организации).

Второй этап: формирование выборочной совокупности сообщений. Если подлежащие анализу случаи (сообщения) немногочисленны и хорошо доступны для исследователя, в ходе проведения контент-анализа изучается вся определенная на первом этапе совокупность источников. Однако в большинстве случаев контент-анализ должен опираться на ограниченную выборку сообщений, взятую из большего массива информации.

Третий этап: выявление единиц анализа – устойчиво повторяющихся смысловых единиц текста, относительно которых выявляются статистические и структурные связи с другими единицами, а также определяются иные количественные или качественные характеристиками.

За единицу анализа могут быть приняты:

- слово;
- предложение;
- тема (идея);
- автор;
- персонаж;
- социальная ситуация;
- часть текста, объединенная чем-то, что соответствует смыслу категории анализа.

К выбору возможной единицы контент-анализа предъявляются следующие **требования**:

- единица анализа должна быть достаточно большой, чтобы выражать какое-либо смысловое значение;
- единица анализа должна быть достаточно малой, чтобы не выражать много (несколько) смысловых значений;
- единица анализа должна легко идентифицироваться;
- число единиц в анализируемом массиве данных должно быть достаточно велико, чтобы из них можно было делать выборку.

Четвертый этап: выделение единиц счета, совпадающих со смысловыми единицами или носящих специфический характер. В первом случае процедура сводится к подсчету частоты упоминания выделенной смысловой единицы в анализируемом тексте. Во втором случае исследователь на основе общих характеристик анализируемого материала и так называемого здравого смысла (собственного профессионализма) сам выдвигает единицы счета, которыми могут быть:

- физическая протяженность текстов;
- площадь текста, заполненная смысловыми единицами;
- число строк (абзацев, знаков, колонок текста);
- длительность трансляции по радио или на телевидении;
- метраж пленки при аудио- и видеозаписях,
- количество рисунков с определенным содержанием, сюжетом и пр.

Пятый этап: процедура непосредственного подсчета оговоренных единиц, аналогичная в общем виде стандартным приемам классификации по выделенным группировкам. На данном этапе применяются специально составленные таблицы, компьютерные программы, оригинальные формулы, статистические расчеты и т.п.

Шестой этап: интерпретация полученных результатов в соответствии с целями и задачами конкретного исследования. На данном этапе выявляются и оцениваются характеристики текстового материала, позволяющие делать заключения о том, что хотел подчеркнуть или скрыть автор анализируемого материала. В ходе интерпретации результатов также возможно определение процента распространенности в обществе субъективных смыслов объекта исследования или анализируемого явления.

Виды контент-анализа, применяемого в конкурентной разведке, представлены на рис. 25.

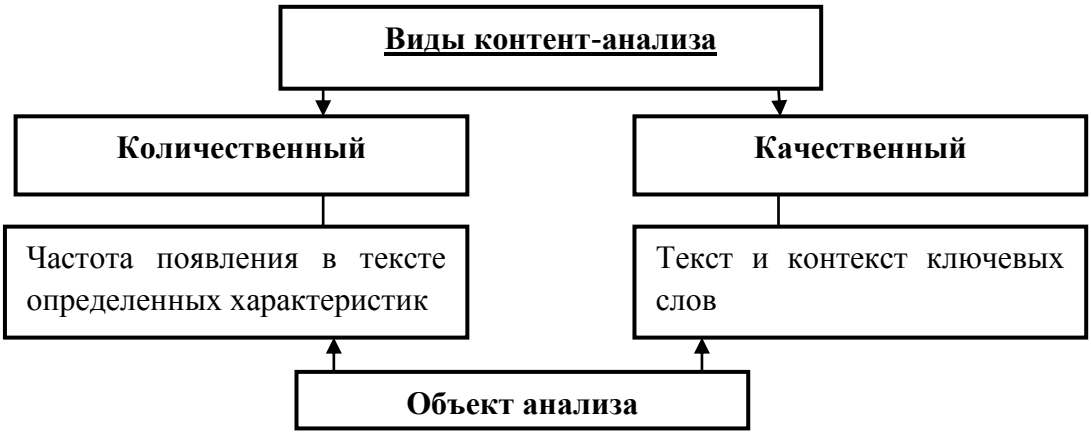

Рис. 25. Виды контент-анализа в конкурентной разведке

Задачи конкурентной разведки, решаемые с помощью контент-анализа:

- определение характера внимания, уделяемого одной и той же теме несколькими изданиями;

- контроль за изменением информационной нагрузки на определенную смысловую категорию.

Достоинства контент-анализа текстовых документов:

- метод требует привлечения относительно небольшого количества трудовых и финансовых ресурсов;
- позволяет оперативно получать фактографические данные о работающих на целевых рынках предприятиях (организациях) в целом, а также о производимых ими товарах и услугах, о их сотрудниках, конкурентных преимуществах, технологиях и т.п.;
- полученная по результатам контент-анализа информация носит объективный характер;
- метод позволяет получать ретроспективный обзор информации об уже прошедших событиях, полевые исследования которых уже невозможны;
- исследовательско - аналитический процесс проведения контент-анализа не оказывает существенного воздействия на объект исследования;
- материалы, используемые службой конкурентной разведки для проведения контент-анализа, являются легкодоступными и относительно дешевыми, т. к. содержатся в открытых источниках - в СМИ;
- в настоящее время проведение контент-аналитического исследования может проводится с широким привлечением современных технических (в том числе – компьютерных) средств и технологий, что в свою очередь значительно сокращает время выполнения анализа и повышает его качество и достоверность;
- текстовые документы, с которыми работает в ходе анализа специалист, не могут «приспосабливаться» к требованиям и ожидаемым результатам исследователя, т.к. их основная масса бывает создана до начала контент-анализа, следовательно – независимо от интересов службы конкурентной разведки.

Недостатки контент-анализа текстовых документов:

- ограниченность количества сообщений, относящихся к изучаемой теме;
- нерегулярность освещения конкретных тем в СМИ;
- быстрое устаревание части информации, содержащейся в анализируемых документах;
- периодическая необходимость проверки достоверности (качества) учетной и отчетной информации, используемой в ходе проведения анализа;
- несовпадение цели написания анализируемого материала в СМИ с задачами службы конкурентной разведки, проводящей контент-анализ, что требует дополнительной «переработки» информации, содержащейся в публикациях;
- наличие обязательного специального требования к исследователю: требование незаурядных воображения и изобретательности;

- контент-анализом текстовых документов служба конкурентной разведки может ограничиться только в случае, когда для решения стоящих перед подразделением задач достаточно фактографической информации;
- факты, содержащиеся в анализируемых текстах, могут быть неполными, фрагментарными, изложенными с использованием заведомо «ангажированного» ракурса;
- используемые при проведении анализа данные относятся исключительно к уже прошедшим событиям и, следовательно, к соответствующим им периодам времени.

Адаптированный алгоритм проведения контент-анализа службой конкурентной разведки предприятия (организации):

- формулировка задачи;
- определение выборки;
- определение единого семантического (смыслового) толкования ключевых понятий;
- составление кода и перечня характеристик текста, обеспечивающих решение поставленной задаче исследования;
- составление регистрационной карточки, протокола контент-анализа и инструкции кодировщику;
- разработка схемы (системы) исследования;
- компьютерная обработка данных;
- предъявление результатов исследовния.

Помимо контент-анализа при работе со СМИ специалисты службы конкурентной разведки используют методы традиционного и формализованного анализа.

Традиционный анализ – это цепочка умственных, логических построений, направленных на выявление сути анализируемого материала с определенной, интересующей аналитика в каждом конкретном случае точки зрения.

Интересующая специалиста информация, содержащаяся в материалах СМИ, обычно присутствует в форме, отвечающей редакционным целям, стоящим перед изданием на момент написания исследуемого материала, что не всегда совпадает с задачами службы конкурентной разведки. Проведение традиционного анализа означает преобразование первоначальной формы этой информации в необходимую исследователю форму, что по сути можно трактовать как её толкование.

Традиционный анализ позволяет улавливать основные мысли и идеи, содержащиеся в исследуемой информации, выясняет логику их обоснования, взвешивает вытекающие из них следствия, выявляет логические связи и логические противоречия между соответствующими постулатами, оценивает их с точки зрения конкурентных позиций. Основным недостатком традиционного анализа является его субъективность.

Формализованный или количественный анализ оперирует конкретными, количественно измеряемыми параметрами. Суть этих методов сводится к поиску таких признаков, черт, свойств анализируемого документа, которые с необходимостью отражали бы определенные существенные стороны его содержания. Это делает качественное содержание документа измеримым, оно становится доступным точным вычислительным операциям. Результаты формализованного анализа являются в достаточной степени объективными. Ограниченность количественного анализа заключается в том, что не все содержание исследуемого документа может быть измерено с помощью формальных показателей. Его основным недостатком следует считать неточное, не исчерпывающее раскрытие содержания документа. В общем случае контент-анализ можно считать частным случаем формализованного анализа.

3.6. Аналитическая разведка средствами интернета

Интернет — всемирная система объединённых компьютерных сетей для хранения и передачи информации.

Характеристики интернета как важнейшего современного источника информации:

- оперативность получения информации, хотя и в неполном объёме;
- достаточность получаемого в интернете объёма информации для первого этапа информационного поиска;
- существование у полученной в интернете информации возможности уточнять дальнейшие поисковые запросы и задавать ориентиры для дальнейших поисков необходимых данных.

На сегодняшний день глобальный интернет можно условно разделить на две части:

- «видимый» интернет: та часть информационных ресурсов, содержимое которой может быть найдено (обнаружено) с помощью поисковых машин;
- «невидимый» интернет: основная часть информационных ресурсов киберпространства, к которым можно получить доступ, если знать, где эти ресурсы находятся, но с помощью поисковых машин найти содержимое ресурсов «невидимого» интернета нельзя.

Основные причины существования «невидимого» интернета:

- физические ограничения скорости: сегодня поисковые машины работают медленнее, чем в интернете появляются новые и исчезают старые информационные страницы;
- высокая стоимость поиска информации: т.к. содержать серверы, рассылать «пауков» («паук» - программа, которая посещает заданные ему сайты, сохраняет их копию в своей базе данных, а потом перемещает эти данные в хранилище), индексировать и исключать сдвоенную информа-

цию дорого, владельцы поисковых машин вводят собственные дополнительные ограничения в работе своих систем;

➢ принцип индексации страниц при помощи «пауков»: если на какую-либо страницу никто не ссылался, а также никто о ней не сообщал поисковой системе вручную, то она не будет проиндексирована; так как посещение страниц «пауками» проходит с заданной периодичностью, изменения, происходящие в промежутке между этими посещениями, некоторое время будут недоступны поисковой системе;

➢ наличие необычных слов на странице, интересующей пользователя: нужная пользователю страница может содержать слова, не совпадающие с теми, что были введены в поисковую машину;

➢ ориентация поисковых машин на скорость поиска, а не на его глубину: поисковая машина обычно ориентирована на наиболее быстрое получение результатов, даже в ущерб полноте поиска; в этом случае не исследуются страницы, индексирование которых трудоемко;

➢ ориентация поисковых машин исключительно на анализ текстов в разных вариантах: поисковые машины сегодня работают только с текстами в различных форматах, не индексируя изображения и звуковые файлы;

➢ разные типы контента (контент – это содержимое сайта, а сайт - это оформление, оболочка данного содержания и одновременно удобный для восприятия макет; контенты бывают текстовые, графические, медиа, в виде аудио- и видеозаписей): разные типы контента могут стать частью невидимого интернета по причинам:

- информация слишком быстро устаревает или изменяется (например, прогноз погоды в реальном времени);
- страница состоит преимущественно из документов в форматах, которые не поддерживаются поисковыми машинами (например, только изображения);
- содержимое страницы генерируется по запросу (например, расчет цены автомобиля в зависимости от комплектации и материала отделки салона);
- содержимое баз данных (результат из базы данных) появляется только после ввода определенного запроса в форму обращения к базе данных;
- страница не вводилась в форму добавления сайта и к ней не ведут никакие ссылки.

Исследовательская работа в интернете может быть организована как самой службой конкурентной разведки предприятия (организации), так и с использованием сторонних организаций.

Риском конкурентной разведки через интернет является наличие для третьих лиц возможности отслеживать информационные запросы конкретного хозяйствующего субъекта, что, в свою очередь, позволяет уста-

новить соответствующую причинно-следственную связь и выявить намерения самого предприятия (организации).

Этапы конкурентной разведки средствами интернет:

- предварительный подбор неструктурированной информации неявного характера в интернете;
- аналитическая обработка полученных массивов данных.

Характеристика отдельных направлений работы службы конкурентной разведки предприятия (организации) в интернете приведена ниже.

С помощью бесплатных поисковых систем общего назначения можно осуществлять следующие **виды работы с интернет-информацией**:

- поиск необходимой исследователю информации по одному или нескольким ключевым словам;
- морфологический поиск информации, т.е. поиск по ключевым словам не только в заданной исследователем форме но и во всех возможных морфологических (грамматических) формах этих слов;
- ранжирование найденных документов по степени их соответствия запросу.

Качество результата поиска информации по запросу, базирующемуся на заданных исследователем ключевых словах, зависит:

- от степени соответствия ключевого слова (фразы) из запроса поставленной исследователем информационной задаче с учетом наличия у поисковой системы возможности уточнять формулировку запроса в ходе выполнения поставленной задачи;
- от характеристик алгоритмов поиска и ведения каталога индексации в конкретной поисковой системе.

Основные недостатки бесплатной информации и бесплатных поисковых систем:

- негарантированная полнота получаемой информации;
- неизвестный уровень достоверности получаемой информации;
- большие затраты времени на получение запрашиваемой информации.

Наиболее популярными в России в настоящее время являются поисковые системы «Яндекс» и «Гугл», которые характеризуются постоянным мониторингом интернета и соответствующей актуализацией собственных информационных баз.

Современные поисковые системы имеют разные алгоритмы сбора и индексации информации. Поэтому для получения максимального количества исходных данных для камеральной работы сотрудник службы конкурентной разведки должен направлять запросы нескольким поисковикам в ходе решения одной задачи. Применение такого подхода к сбору информации с помощью поисковых систем в интернете позволяет значительно повышать эффективность последующей работы специалиста с собранной информацией.

Сегодня лучшие поисковые системы умеют в ходе работы над запросом не только искать запрашиваемую информацию, но и ставить «фильтры» для изъятия из результатов поиска так называемый спам (спам – это ненужные адресату электронные послания, рекламные письма и т.п., рассылаемые отдельными фирмами по интернету или электронной почте).

Сократить количество предлагаемой системой как результат поиска по запросу информации можно с помощью функции «Расширенный поиск», позволяющей проводить её (информации) первоначальную фильтрацию до начала непосредственно поиска путём максимальной конкретизации формулировки запроса. В этом случае запрос может включать в себя не только набор ключевых слов, но и тип файла (например, Word или Excel), адрес анализируемого файла и т.п.

Дополнительные возможности, предоставляемые поисковыми системами пользователю для повышения скорости и точности поиска, представлены на рис. 26.

Рис. 26. Дополнительные возможности поисковых систем

Способы сортировки результатов поиска:

- по степени соответствия запросу полученных результатов;
- по дате последнего изменения документа.

Служба конкурентной разведки бывает заинтересована в своевременной актуализации результатов поиска. Такую возможность предоставляет функция соответствующего мониторинга, осуществляемая с помощью специального программного обеспечения («сторожевых роботов»), позволяющего

сохранить образ информационного файла в базе данных, а при повторном его посещении – сравнить актуальное состояние ресурса с этим образом.

На рис. 27 приведены информационные ресурсы интернета, используемые службой конкурентной разведки предприятия (организации).

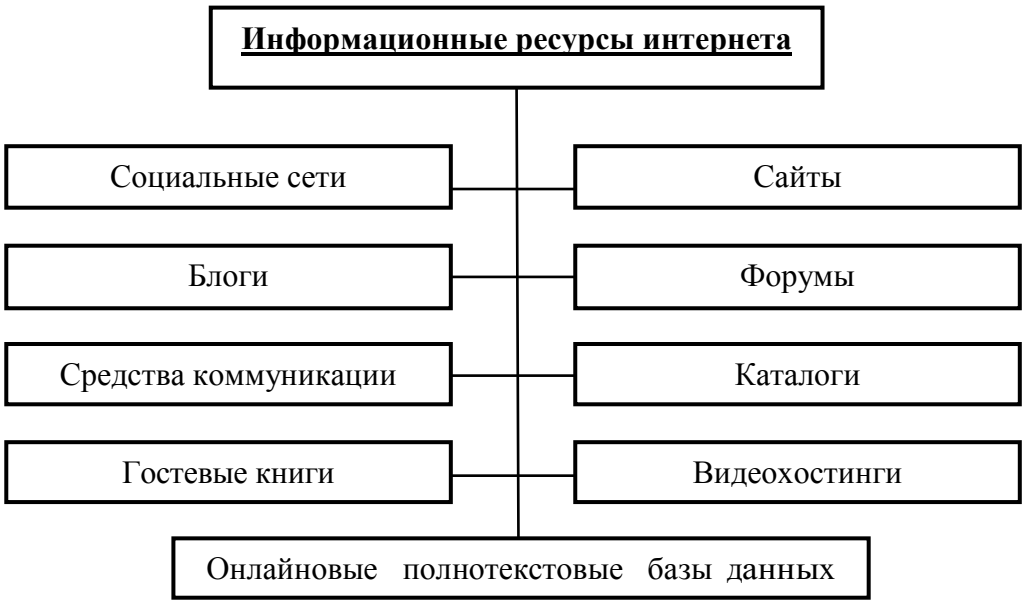

Рис. 27. Информационные ресурсы интернета

Общая характеристика информационных ресурсов интернета и содержащейся в них информации, интересной для службы конкурентной разведки предприятия (организации) представлена ниже.

Социальные сети – это платформы, онлайн-сервисы и веб-сайты, предназначенные для построения, отражения и организации социальных взаимоотношений в Интернете.

Для службы конкурентной разведки предприятия (организации) социальные сети – это источник информации о конкретных людях, а также возможность установления связей с интересующим объектом без привлечения нежелательного внимания. В них содержится информация, позволяющая определить статус человека (результат анализа списка друзей), его материальное положение (результат анализа фотографии летнего отдыха), некоторые персональные данные (дату рождения, образование, место проживания, место работы и т.п.) и его увлечения. В результате специалист конкурентной разведки может составить предварительный психологический портрет изучаемого объекта и наметить направления дальнейших действий по его использованию с целью получения информации. Изучение контактов человека также позволяет понять, через кого и с использованием какого повода можно установить личный контакт с ним.

Сайт – это совокупность страниц, объединенных одной общей темой, дизайном, имеющих взаимосвязанную систему ссылок, расположенных в сети интернет.

Для специалистов конкурентной разведки наибольший интерес представляют интернет-сайты изучаемых хозяйствующих, на которых может размещаться информация о структуре предприятий (организаций), их история, сфера деятельности, крупные реализованные проекты, информация о выпускаемых товарах (оказываемых услугах) и т.д. Аналогичная информация может размещаться также на новостных и региональных порталах, форумах, блогах, в социальных сетях.

После изучения содержания соответствующих сайтов специалисты конкурентной разведки могут смоделировать:

✓ планы хозяйствующих субъектов (например, исходя из текста доклада руководителя на общем собрании акционеров);

✓ некоторые перспективные направления деятельности хозяйствующих субъектов (например, исходя из появления в исходном коде страницы новых ключевых слов);

✓ конфиденциальные документы хозяйствующих субъектов (например, исходя в ходе анализа структуры адресов документов можно обнаружить скрытые документы с открытым доступом к ним) и т.д.

Блоги – это специальным образом организованные интернет-сайты, позволяющие его владельцу и лицам, получившим специальный допуск, вести на страницах сайта записи в режиме дневника в хронологическом порядке. По авторскому составу блоги могут быть личными (индивидуальными), групповыми (корпоративными, клубными и т. д.) и общественными.

Блогосфера – это глобальная база всех блогов интернета, предназначенных для поиска и обмена информацией, формирования и высказывания личностных и коллективных мнений. Взаимодействие между блогерами (владельцами собственного блога) происходит за счет комментариев, гиперссылок, записей, оперативного размещения новостей, что, в свою очередь, позволяет информации распространяться в сети интернет с очень высокой скоростью. Она представляет собой разветвленное сетевое мегасообщество, на сегодняшний день являющееся не только средством массовой информации, но и источником информации для традиционных СМИ.

Направления использования блогосферы в конкурентной разведке:

➢ установление контакта с интересующим человеком путём размещения комментариев в его блоге в соответствии с эмоциональными ожиданиям объекта исследования (похвалы, восхищение, согласие с позицией автора, критика его оппонентов, аргументированная полемика и т.п.);

➢ поиск информации о людях, не ведущих собственных блогов, но размещающих в блогосфере свои комментарии, или являющихся тематическими персонажами в записях сторонних блогеров;

➢ сбор дополнительных сведений о претендентах на вакантную должность и контроль настроений работающего персонала предприятия (организации).

Форумы – это специальные сайты, предназначенные для онлайн-

общения пользователей и имеющие структуру, состоящую из разделов, тем (веток) и сообщений (постов). Разделы обычно не меняют своего местоположения на форуме относительно друг друга, а перечень тем постоянно актуализируется вслед за появлением в них свежих сообщений. Новые темы для обсуждения может создавать не только администратор (или владелец) ресурса, но и любой пользователь.

Использование интернет–форумов службой конкурентной разведки предприятий (организаций) аналогично работе специалистов в блогосфере. К числу дополнительных возможностей форумов относятся:

- возможность идентификации лиц (физических и юридических), организующих информационную атаку на человека или хозяйствующий субъект и, при благоприятном стечении обстоятельств, - возможность прекратить эту атаку;
- возможность изменить отношение целевой аудитории к любому хозяйствующему субъекту (включая собственный), используя формат «вопрос – ответ».

Особенности работы с информацией, получаемой на интернет-форумах:

- вся интересующая службу конкурентной разведки информация должна быть своевременно скопирована в собственную информационную базу, т.к. темы на форумах модерируются администратором и со временем удаляются;
- всю полученную информацию необходимо поверять, т.к. уровень её достоверности не подтверждается никакими обязательствами со стороны лица, размещающего её на страницах форума.

Средства интернет-коммуникации – это такие методы общения, при которых передача информации происходит по каналам интернет с использованием стандартных протоколов обмена и представления информации. Информация может передаваться в различной форме - голос, видео, документы, мгновенные сообщения, файлы. Они обеспечивают связь между людьми и хозяйствующими субъектами (ICQ, Skype, электронная почта и т.д.) и используются в конкурентной разведке для идентификации объектов анализа. Такая возможность обусловлена тем, что пользователи размещают свои регистрационные коммуникационные номера в социальных сетях, на официальных сайтах предприятий (организаций), в личных объявлениях и т.п. Таким образом, соответствующий регистрационный номер объекта анализа может выступать в качестве ключевого слова при работе поисковых машин по соответствующим запросам специалистов конкурентной разведки.

Каталог – это, в общем случае, некий список информации об объектах, составленный с целью облегчения поиска этих объектов по какому-то признаку. Применительно к сети интернет каталог (директория, справочник, папка) — это объект в файловой системе, упрощающий организацию

файлов; это рубрикатор или классификатор, организующий документы по принципу дерева. Для эффективного использования каталога нужно знать принцип построения его структуры. При работе с каталогами необходимо учитывать, что для каждого из них разработана своя индексация, поэтому один и тот же запрос может дать разные результаты.

Классификация каталогов:

- каталоги общей направленности;
- специализированные каталоги, позволяющие пользователям ориентироваться в узкоспециализированных темах.

Каталоги используются службой конкурентной разведки в качестве оперативного интернет-помощника, позволяющего повысить скорость сбора информации по заданным темам.

Гостевые книги – это один из разделов сайта хозяйствующего субъекта, в котором посетители могут оставлять свои записи. Они представляют собой ленту не приспособленных к диалогу и плохо структурированных сообщений в формате «вопрос – ответ». Однако информация, размещаемая в гостевых книгах, представляет собой совокупность публичных данных, поступающих в адрес предприятия (организации) по открытому каналу обратной связи и позволяющих судить об отношении к нему третьих лиц, являющихся различными субъектами рынка. Анализ данной информации позволяет службе конкурентной разведке получать достаточно объективную характеристику рыночной позиции анализируемых рыночных игроков.

Видеохостинги – сайты, предназначены для размещения авторизованными пользователями видеороликов с разными вариантами доступа к материалам **(хо́стинг –** услуга по предоставлению ресурсов для размещения информации на сервере, постоянно находящемся в интернете).

Использование видеохостингов службой конкурентной разведки предприятий (организаций) аналогично работе специалистов в блогосфере.

Онлайновые полнотекстовые базы данных формируются информационными агентствами и консалтинговыми организациями, отвечающими за качество содержащейся в них информации своей репутацией. Информация, содержащаяся в этих базах, является платной.

У вышеперечисленных организаций хорошо налажен анализ центральной (но не региональной) прессы. При работе с базами данных пользователи могут самостоятельно работать со всем объемом содержащейся в них информации, а могут за дополнительную плату воспользоваться услугами штатных аналитиков. Также аналитические и информационные агентства предоставляют услуги оперативного мониторинга СМИ по любой теме, тематическую подборку публикаций, регулярные тематические обзоры прессы. Для службы конкурентной разведки онлайновые полнотекстовые базы данных являются источником достоверной, но не эксклюзивной информации.

3.7. Работа с людьми

Отдельный человек может быть источником (носителем, обладателем) информации, необходимой третьему лицу**.** Поэтому в конкурентной разведке есть методы поиска такого человека и получения от него нужной информации.

Каждый человек обладает информацией, часть которой никогда и нигде не будет опубликована. Люди умеют хранить, обрабатывать, передавать информацию, могут восполнять недостающие куски информации и порождать новую информацию путем анализа имеющейся. Часто люди обнародуют ценную для конкурентной разведки информацию, даже не понимая, что последняя может представлять для кого-то реальную ценность. Именно работа с людьми – **основа работы конкурентной разведки**, остальные инструменты по отношению к работе с людьми играют вспомогательную роль.

Информация, полученная непосредственно от отдельного человека рассматривается как **информации из открытого источника**, т.к. этот источник никем и ничем не закрыт, если речь не идёт о государственной, коммерческой тайне или закрытых (персональных) данных.

Допустимо, если исследователь в разговоре с объектом исследования коснется вопросов, составляющих, например, чужую коммерческую тайну, т.к. исследователь может не знать о «засекреченности» той или иной темы. В этом случае именно отвечающий должен добровольно решить, что и как ему говорить в ответ на поставленный вопрос. Если же в разговоре речь идет о третьей стороне, то говорить о коммерческой тайне некорректно, так как ни специалист конкурентной разведки, ни его собеседник не являются носителями коммерческой тайны посторонних для них юридических и физических лиц. Данный вопрос регулируется не законом, а этикой.

Работа с людьми является самой деликатной частью работы службы конкурентной разведки, т.к. именно в этой области проще всего перейти грань между конкурентной разведкой и промышленным шпионажем.

Направления работы с людьми в конкурентной разведке:

- разовые контакты;
- выстраивание долгосрочных отношений.

Алгоритм работы с конкретным человеком как объектом разведывательной операции специалист конкурентной разведки разрабатывает каждый раз индивидуально, с учетом:

- целей и задач конкретного исследования;
- объективных и субъективных характеристик человека, являющегося объектом исследования;
- персональных характеристик как исследования, так и самого исследователя.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Федеральный закон РФ от 21 июня 1993г. № 5485-I «О государственной тайне»;

2. Федеральный закон РФ от 29 июля 2004 г. N 98-ФЗ «О коммерческой тайне»;

3. Федеральный закон РФ от 27 июля 2006 года 152-ФЗ «О персональных данных»;

4. Федеральный закон РФ от 11 марта 1992 г. N 2487-I «О частной детективной и охранной деятельности в Российской Федерации»;

5. Конкурентная разведка: учебное пособие. Ч.1 / под ред. Е.Л. Ющука, А.А. Мальцева. – Екатеринбург: Изд-во Уральского государственного экономического университета. – 2015. – 210 с.;

6. Подоляк О.О. Конкурентная разведка: учебное пособие / О.О. Подоляк, Е.Ю. Кузнецова. – Екатеринбург: УрФУ, – 2012. – 93 стр.

7. Теория и практика конкуренции. Учебник для студентов 3 курса экономических специальностей / под ред. Рубина Ю.Б. Московский государственный университет экономики, статистики и информатики. – М., 2001 – 428 с.

8. http://www.leader-hr.ru;

9. http://www.Grandars.ru;

10. http://www.snabjenci.ru.

ПРИЛОЖЕНИЯ

Приложение А

Федеральный закон № 5485-I «О государственной тайне»

Закон Российской Федерации «О государственной тайне» от 21 июня 1993 г. № 5485-I (с изменениями и дополнениями от 6 октября 1997 г. № 131-ФЗ; от 30 июня 2003 г. № 86-ФЗ; от 11 ноября 2003 г. № 153-ФЗ; от 29 июня 2004 г. № 58-ФЗ; от 22 августа 2004 г. № 122-ФЗ)

Настоящий Закон регулирует отношения, возникающие в связи с отнесением сведений к государственной тайне, их засекречиванием или рассекречиванием и защитой в интересах обеспечения безопасности Российской Федерации. (В редакции Федерального закона от 6 октября 1997 г. № 131-ФЗ)

Раздел I Общие Положения

Статья 1. Сфера действия настоящего Закона

Положения настоящего Закона обязательны для исполнения на территории Российской Федерации и за ее пределами органами законодательной, исполнительной и судебной властей (далее – органы государственной власти), местного самоуправления, предприятиями, учреждениями и организациями независимо от их организационно-правовой формы и формы собственности, должностными лицами и гражданами Российской Федерации, взявшими на себя обязательства либо обязанными по своему статусу исполнять требования законодательства Российской Федерации о государственной тайне.

Статья 2. Основные понятия, используемые в настоящем Законе

В настоящем Законе используются следующие основные понятия:

- государственная тайна – защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации;
- носители сведений, составляющих государственную тайну, – материальные объекты, в том числе физические поля, в которых сведения, составляющие государственную тайну, находят свое отображение в виде символов, образов сигналов, технических решений и процессов;
- система защиты государственной тайны – совокупность органов защиты государственной тайны, используемых ими средств и методов защиты сведений, составляющих государственную тайну и их носителей, а также мероприятий, проводимых в этих целях;
- допуск к государственной тайне – процедура оформления права граждан на доступ к сведениям, составляющим государственную тайну, а предприятий, учреждений и организаций – на проведение работ с использованием таких сведений;
- доступ к сведениям, составляющим государственную тайну, – санкционированное полномочным должностным лицом ознакомление конкретного лица со сведениями, составляющими государственную тайну;
- гриф секретности – реквизиты, свидетельствующие о степени секретности сведений, содержащихся в их носителе, проставляемые на самом носителе и (или) в сопроводительной документации на него;
- средства защиты информации – технические, криптографические, программные и другие средства, предназначенные для защиты сведений, составляющих государственную тайну, средства, в которых они реализованы, а также средства контроля эффективности защиты информации.

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

(**Статья 3. Законодательство Российской Федерации о государственной тайне**

Законодательство Российской Федерации о государственной тайне основывается на Конституции Российской Федерации, Законе Российской Федерации "О безопасности" и включает настоящий Закон, а также положения других актов законодательства, регулирующих отношения, связанные с защитой государственной тайны.

Статья 4. Полномочия органов государственной власти и должностных лиц в области отнесения сведений к государственной тайне и их защиты

1. Палаты Федерального Собрания:

- осуществляют законодательное регулирование отношений в области государственной тайны;
- рассматривают статьи федерального бюджета в части средств, направляемых на реализацию государственных программ в области защиты государственной тайны;
- определяют полномочия должностных лиц в аппаратах палат Федерального Собрания по обеспечению защиты государственной тайны в палатах Федерального Собрания;

2. Президент Российской Федерации:

- утверждает государственные программы в области защиты государственной тайны;
- утверждает по представлению Правительства Российской Федерации состав, структуру межведомственной комиссии по защите государственной тайны и положение о ней;
- утверждает по представлению Правительства Российской Федерации Перечень должностных лиц органов государственной власти, наделяемых полномочиями по отнесению сведений к государственной тайне, а также Перечень сведений, отнесенных к государственной тайне;
- заключает международные договоры Российской Федерации о совместном использовании и защите сведений, составляющих государственную тайну;
- определяет полномочия должностных лиц по обеспечению защиты государственной тайны в Администрации Президента Российской Федерации;
- в пределах своих полномочий решает иные вопросы, возникающие в связи с отнесением сведений к государственной тайне, их засекречиванием или рассекречиванием и их защитой.

3. Правительство Российской Федерации:

- организует исполнение Закона Российской Федерации «О государственной тайне»;
- представляет на утверждение Президенту Российской Федерации состав, структуру межведомственной комиссии по защите государственной тайны и положение о ней;
- представляет на утверждение Президенту Российской Федерации Перечень должностных лиц органов государственной власти, наделяемых полномочиями по отнесению сведений к государственной тайне;
- устанавливает порядок разработки Перечня сведений, отнесенных к государственной тайне;
- организует разработку и выполнение государственных программ в области защиты государственной тайны;
- определяет полномочия должностных лиц по обеспечению защиты государственной тайны в аппарате Правительства Российской Федерации;
- устанавливает порядок предоставления социальных гарантий гражданам, допущенным к государственной тайне на постоянной основе, и сотрудникам структурных подразделений по защите государственной тайны;

- устанавливает порядок определения размеров ущерба, наступившего в результате несанкционированного распространения сведений, составляющих государственную тайну, а также ущерба, наносимого собственнику информации в результате ее засекречивания;
- заключает межправительственные соглашения, принимает меры по выполнению международных договоров Российской Федерации о совместном использовании и защите сведений, составляющих государственную тайну, принимает решения о возможности передачи их носителей другим государства;
- в пределах своих полномочий решает иные вопросы, возникающие в связи с отнесением сведений к государственной тайне, их засекречиванием или рассекречиванием и их защитой.

4. Органы государственной власти Российской Федерации, органы государственной власти субъектов Российской Федерации и органы местного самоуправления во взаимодействии с органами защиты государственной тайны, расположенными в пределах соответствующих территорий:

- обеспечивают защиту переданных им другими органами государственной власти, предприятиями, учреждениями и организациями сведений, составляющих государственную тайну, а также сведений, засекречиваемых ими;
- обеспечивают защиту государственной тайны на подведомственных им предприятиях, в учреждениях и организациях в соответствии с требованиями актов законодательства Российской Федерации;
- устанавливают размеры предоставляемых социальных гарантий гражданам, допущенным к государственной тайне на постоянной основе, и сотрудникам структурных подразделений по защите государственной тайны на подведомственных им предприятиях, в учреждениях и организациях;
- обеспечивают в пределах своей компетенции проведение проверочных мероприятий в отношении граждан, допускаемых к государственной тайне;
- реализуют предусмотренные законодательством меры по ограничению прав граждан и предоставлению социальных гарантий лицам, имеющим либо имевшим доступ к сведениям, составляющим государственную тайну;
- вносят в полномочные органы государственной власти предложения по совершенствованию системы защиты государственной тайны.

5. Органы судебной власти:

- рассматривают уголовные и гражданские дела о нарушениях законодательства Российской Федерации о государственной тайне;
- обеспечивают судебную защиту граждан, органов государственной власти, предприятий, учреждений и организаций в связи с их деятельностью по защите государственной тайны;
- обеспечивают в ходе рассмотрения указанных дел защиту государственной тайны;
- определяют полномочия должностных лиц по обеспечению защиты государственной тайны в органах судебной власти.

Раздел II Перечень сведений, составляющих государственную тайну

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;
- о запасах платины, металлов платиновой группы, природных алмазов в Государственном фонде драгоценных металлов и драгоценных камней Российской Федерации, Центральном банке Российской Федерации, а также об объемах запасов в недрах, добычи, производства и потребления стратегических видов полезных ископаемых Российской Федерации (по списку, определяемому Правительством Российской Федерации);

3) сведения в области внешней политики и экономики:

- о внешнеполитической, внешнеэкономической деятельности Российской Федерации, преждевременное распространение которых может нанести ущерб безопасности государства;
- о финансовой политике в отношении иностранных государств (за исключением обобщенных показателей по внешней задолженности), а также о финансовой или денежно-кредитной деятельности, преждевременное распространение которых может нанести ущерб безопасности государства;

4) сведения в области разведывательной, контрразведывательной и оперативно-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.

Раздел III Отнесение сведений к государственной тайне и их засекречивание

Статья 6. Принципы отнесения сведений к государственной тайне и засекречивания этих сведений

Отнесение сведений к государственной тайне и их засекречивание - введение в предусмотренном настоящим Законом порядке для сведений составляющих государственную тайну, ограничений на их распространение и на доступ к их носителям.

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

Законность отнесения сведений к государственной тайне и их засекречивания заключается в соответствии засекречиваемых сведений положениям статей 5 и 7 настоящего Закона и законодательству Российской Федерации 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.

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 социальных гарантиях, 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.

Статья 8. Степени секретности сведений и грифы секретности носителей этих сведений

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

Устанавливаются три степени секретности сведений, составляющих государственную тайну, и соответствующие этим степеням грифы секретности для носителей указанных сведений: «особой важности», «совершенно секретно» и «секретно».

Порядок определения размеров ущерба, который может быть нанесен безопасности Российской Федерации вследствие распространения сведений, составляющих государственную тайну и правила отнесения указанных сведений к той или иной степени секретности устанавливаются Правительством Российской Федерации.

Использование перечисленных грифов секретности для засекречивания сведений, не отнесенных к государственной тайне, не допускается.

Статья 9. Порядок отнесения сведений к государственной тайне

Отнесение сведений к государственной тайне осуществляется в соответствии с их отраслевой, ведомственной или программно-целевой принадлежностью, а также в соответствии с настоящим Законом.

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

Отнесение сведений к государственной тайне осуществляется в соответствии с Перечнем сведений, составляющих государственную тайну, определяемым настоящим Законом, руководителями органов государственной власти в соответствии с Перечнем

должностных лиц, наделенных полномочиями по отнесению сведений к государственной тайне, утверждаемым Президентом Российской Федерации. Указанные лица несут персональную ответственность за принятые ими решения о целесообразности отнесения конкретных сведений к государственной тайне.

Для осуществления единой государственной политики в области засекречивания сведений межведомственная комиссия по защите государственной тайны формирует по предложениям органов государственной власти и в соответствии с Перечнем сведений, составляющих государственную тайну, Перечень сведений, отнесенных к государственной тайне. В этом Перечне указываются органы государственной власти, наделяемые полномочиями по распоряжению данными сведениями. Указанный Перечень утверждается Президентом Российской Федерации, подлежит открытому опубликованию и пересматривается по мере необходимости.

Органами государственной власти, руководители которых наделены полномочиями по отнесению сведений к государственной тайне, в соответствии с Перечнем сведений, отнесенных к государственной тайне, разрабатываются развернутые перечни сведений, подлежащих засекречиванию. В эти перечни включаются сведения, полномочиями по распоряжению которыми наделены указанные органы, и устанавливается степень их секретности. В рамках целевых программ по разработке и модернизации образцов вооружения и военной техники, опытно-конструкторских и научно-исследовательских работ по решению заказчиков указанных образцов и работ могут разрабатываться отдельные перечни сведений, подлежащих засекречиванию. Эти перечни утверждаются соответствующими руководителями органов государственной власти. Целесообразность засекречивания таких перечней определяется их содержанием.

Статья 10. Ограничение прав собственности предприятий, учреждений организаций и граждан Российской Федерации на информацию в связи с ее засекречиванием

Должностные лица, наделенные в порядке, предусмотренном статьей 9 настоящего Закона, полномочиями по отнесению сведений к государственной тайне, вправе принимать решения о засекречивании информации, находящейся в собственности предприятий, учреждений, организаций и граждан (далее - собственник информации), если эта информация включает сведения, перечисленные в Перечне сведений, отнесенных к государственной тайне. Засекречивание указанной информации осуществляется по представлению собственников информации или соответствующих органов государственной власти.

Материальный ущерб, наносимый собственнику информации в связи с ее засекречиванием, возмещается государством в размерах, определяемых в договоре между органом государственной власти, в распоряжение которого переходит эта информация, и ее собственником. В договоре также предусматриваются обязательства собственника информации по ее нераспространению. При отказе собственника информации от подписания договора он предупреждается об ответственности за несанкционированное распространение сведений, составляющих государственную тайну в соответствии с действующим законодательством.

Собственник информации вправе обжаловать в суд действия должностных лиц, ущемляющие, по мнению собственника информации, его права. В случае признания судом действий должностных лиц незаконными порядок возмещения ущерба, нанесенного собственнику информации, определяется решением суда в соответствии с действующим законодательством.

Не может быть ограничено право собственности на информацию иностранных организаций и иностранных граждан, если эта информация получена (разработана) ими без нарушения законодательства Российской Федерации.

Статья 11. Порядок засекречивания сведений и их носителей

Основанием для засекречивания сведений, полученных (разработанных) в результате управленческой, производственной, научной и иных видов деятельности органов государственной власти, предприятий, учреждений и организаций, является их соответствие действующим в данных органах, на данных предприятиях, в данных учреждениях и организациях перечням сведений, подлежащих засекречиванию. При засекречивании этих сведений их носителям присваивается соответствующий гриф секретности.

При невозможности идентификации полученных (разработанных) сведений со сведениями, содержащимися в действующем перечне, должностные лица органов государственной власти, предприятий, учреждений и организаций обязаны обеспечить предварительное засекречивание полученных (разработанных) сведений в соответствии с предполагаемой степенью секретности и в месячный срок направить в адрес должностного лица, утвердившего указанный перечень, предложения по его дополнению (изменению).

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

Статья 12. Реквизиты носителей сведений, составляющих государственную тайну

На носители сведений, составляющих государственную тайну, 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 данных учреждении и организации перечня сведений, подлежащих засекречиванию;
- об органе государственной власти, о предприятии, об учреждении, организации, осуществивших засекречивание носителя;
- о регистрационном номере;
- о дате или условии рассекречивания сведений либо о событии, после наступления которого сведения будут рассекречены.

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

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

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

Раздел IV Рассекречивание сведений и их носителей

Статья 13. Порядок рассекречивания сведений

Рассекречивание сведений и их носителей – снятие ранее введенных в предусмотренном настоящим Законом порядке ограничений на распространение сведений, составляющих государственную тайну, и на доступ к их носителям.

Основаниями для рассекречивания сведений являются:

- взятие на себя Российской Федерацией международных обязательств по открытому обмену сведениями, составляющими в Российской Федерации государственную тайну;
- изменение объективных обстоятельств, вследствие которого дальнейшая защита сведений, составляющих государственную тайну, является нецелесообразной.

Органы государственной власти, руководители которых наделены полномочиями по отнесению сведений к государственной тайне, обязаны периодически, но не реже чем через каждые 5 лет, пересматривать содержание действующих в органах государственной власти, на предприятиях, в учреждениях и организациях перечней сведений, подлежащих засекречиванию, в части обоснованности засекречивания сведений и их соответствия установленной ранее степени секретности.

Срок засекречивания сведений, составляющих государственную тайну, не должен превышать 30 лет. В исключительных случаях этот срок может быть продлен по заключению межведомственной комиссии по защите государственной тайны.

Правом изменения действующих в органах государственной власти, на предприятиях, в учреждениях и организациях перечней сведений, подлежащих засекречиванию, наделяются утвердившие их руководители органов государственной власти, которые несут персональную ответственность за обоснованность принятых ими решений по рассекречиванию сведений. Решения указанных руководителей, связанные с изменением перечня сведений, отнесенных к государственной тайне, подлежат согласованию с межведомственной комиссией по защите государственной тайны, которая вправе приостанавливать и опротестовывать эти решения.

Статья 14. Порядок рассекречивания носителей сведений, составляющих государственную тайну

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

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, учреждений и организаций наделяются полномочиями по рассекречиванию носителей сведений, необоснованно засекреченных подчиненными им должностными лицами.

Руководители государственных архивов Российской Федерации наделяются полномочиями по рассекречиванию носителей сведений, составляющих государственную тайну, находящихся на хранении в закрытых фондах этих архивов, в случае делегирования им таких полномочий организацией-фондообразователем или ее правопреемником. В случае ликвидации организации-фондообразователя и отсутствия ее правопреемника вопрос о порядке рассекречивания носителей сведений, составляющих государ-

ственную тайну, рассматривается межведомственной комиссией по защите государственной тайны.

Статья 15. Исполнение запросов граждан, предприятий, учреждений, организаций и органов государственной власти Российской Федерации о рассекречивании сведений

Граждане, предприятия, учреждения, организации и органы государственной власти Российской Федерации вправе обратиться в органы государственной власти на предприятия в учреждения, организации в том числе в государственные архивы, с запросом о рассекречивании сведений, отнесенных к государственной тайне.

Органы государственной власти, предприятия, учреждения, организации, в том числе государственные архивы, получившие такой запрос, обязаны в течение трех месяцев рассмотреть его и дать мотивированный ответ по существу запроса. Если они не правомочны решить вопрос о рассекречивании запрашиваемых сведений, то запрос в месячный срок с момента его поступления передается в орган государственной власти, наделенный такими полномочиями либо в межведомственную комиссию по защите государственной тайны о чем уведомляются граждане предприятия, учреждения, организации и органы государственной власти Российской Федерации, подавшие запрос.

Уклонение должностных лиц от рассмотрения запроса по существу влечет за собой административную (дисциплинарную) ответственность в соответствии с действующим законодательством.

Обоснованность отнесения сведений к государственной тайне может быть обжалована в суд. При признании судом необоснованности засекречивания сведений эти сведения подлежат рассекречиванию в установленном настоящим Законом порядке.

Раздел V Распоряжение сведениями, составляющими государственную тайну

Статья 16. Взаимная передача сведений, составляющих государственную тайну, органами государственной власти, предприятиями, учреждениями и организациями

Взаимная передача сведений, составляющих государственную тайну, осуществляется органами государственной власти, предприятиями, учреждениями и организациями, не состоящими в отношениях подчиненности и не выполняющими совместных работ с санкции органа государственной власти, в распоряжение которого в соответствии со статьей 9 настоящего Закона находятся эти сведения.

Органы государственной власти, предприятия, учреждения и организации, запрашивающие сведения, составляющие государственную тайну, обязаны создать условия, обеспечивающие защиту этих сведений. Их руководители несут персональную ответственность за несоблюдение установленных ограничений по ознакомлению со сведениями, составляющими государственную тайну.

Обязательным условием для передачи сведений, составляющих государственную тайну, органам государственной власти, предприятиям, учреждениям и организациям является выполнение ими требований, предусмотренных в статье 27 настоящего Закона.

Статья 17. Передача сведений, составляющих государственную тайну, в связи с выполнением совместных и других работ

Передача сведений, составляющих государственную тайну, предприятиям, учреждениям, организациям или гражданам в связи с выполнением совместных и других работ осуществляется заказчиком этих работ с разрешения органа государственной власти, в распоряжении которого в соответствии со статьей 9 настоящего Закона находятся соответствующие сведения, и только в объеме, необходимом для выполнения этих работ. При этом до передачи сведений, составляющих государственную тайну, заказчик обязан убедиться в наличии у предприятия, учреждения или организации лицензии на

проведение работ с использованием сведений соответствующей степени секретности, а у граждан – соответствующего допуска.

Предприятия, учреждения или организации, в том числе и негосударственных форм собственности, при проведении совместных и других работ (получении государственных заказов) и возникновении в связи с этим необходимости в использовании сведений, составляющих государственную тайну, могут заключать с государственными предприятиями, учреждениями или организациями договоры об использовании услуг их структурных подразделений по защите государственной тайны, о чем делается соответствующая отметка в лицензиях на проведение работ с использованием сведений, составляющих государственную тайну, обеих договаривающихся сторон.

В договоре на проведение совместных и других работ, заключаемом в установленном законом порядке, предусматриваются взаимные обязательства сторон по обеспечению сохранности сведений, составляющих государственную тайну, как в процессе проведения работ, так и по их завершении, а также условия финансирования работ (услуг) по защите сведений, составляющих государственную тайну.

Организация контроля за эффективностью защиты государственной тайны при проведении совместных и других работ возлагается на заказчика этих работ в соответствии с положениями заключенного сторонами договора.

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

Статья 18. Передача сведений, составляющих государственную тайну, другим государствам

Решение о передаче сведений, составляющих государственную тайну, другим государствам принимается Правительством Российской Федерации при наличии экспертного заключения межведомственной комиссии по защите государственной тайны о возможности передачи этих сведений.

Обязательства принимающей стороны по защите передаваемых ей сведений предусматриваются заключаемым с ней договором (соглашением).

Статья 19. Защита сведений, составляющих государственную тайну, при изменении функций субъектов правоотношений

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

- правопреемнику органа государственной власти, предприятия, учреждения или организации, располагающих сведениями, составляющими государственную тайну, если этот правопреемник имеет полномочия по проведению работ с использованием указанных сведений;
- органу государственной власти, в распоряжении которого в соответствии со статьей 9 настоящего Закона находятся соответствующие сведения;
- другому органу государственной власти, предприятию, учреждению или организации по указанию межведомственной комиссии по защите государственной тайны.

Раздел VI Защита государственной тайны

Статья 20. Органы защиты государственной тайны

К органам защиты государственной тайны относятся:

- межведомственная комиссия по защите государственной тайны;
- федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности, федеральный орган исполнительной власти, уполномоченный в области обороны, федеральный орган исполнительной власти, уполномоченный в области внешней разведки, федеральный орган исполнительной власти, уполномоченный в области противодействия техническим разведкам и технической защиты информации, и их территориальные органы;
- органы государственной власти, предприятия, учреждения и организации и их структурные подразделения по защите государственной тайны.

Межведомственная комиссия по защите государственной тайны является коллегиальным органом, координирующим деятельность органов государственной власти по защите государственной тайны в интересах разработки и выполнения государственных программ нормативных и методических документов, обеспечивающих реализацию законодательства Российской Федерации о государственной тайне. Функции межведомственной комиссии по защите государственной тайны и ее надведомственные полномочия реализуются в соответствии с Положением о межведомственной комиссии по защите государственной тайны, утверждаемым Президентом Российской Федерации.

Федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности, федеральный орган исполнительной власти, уполномоченный в области обороны, федеральный орган исполнительной власти, уполномоченный в области внешней разведки, федеральный орган исполнительной власти, уполномоченный в области противодействия техническим разведкам и технической защиты информации, и их территориальные органы организуют и обеспечивают защиту государственной тайны в соответствии с функциями, возложенными на них законодательством Российской Федерации.

Органы государственной власти, предприятия, учреждения и организации обеспечивают защиту сведений, составляющих государственную тайну, в соответствии с возложенными на них задачами и в пределах своей компетенции. Ответственность за организацию защиты сведений, составляющих государственную тайну, в органах государственной власти, на предприятиях в учреждениях и организациях возлагается на их руководителей. В зависимости от объема работ с использованием сведений, составляющих государственную тайну, руководителями органов государственной власти предприятий, учреждений и организаций создаются структурные подразделения по защите государственной тайны, функции которых определяются указанными руководителями в соответствии с нормативными документами, утверждаемыми Правительством Российской Федерации, и с учетом специфики проводимых ими работ.

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

Статья 21. Допуск должностных лиц и граждан к государственной тайне

Допуск должностных лиц и граждан Российской Федерации к государственной тайне осуществляется в добровольном порядке.

Допуск лиц, имеющих двойное гражданство, лиц без гражданства, а также лиц из числа иностранных граждан, эмигрантов и реэмигрантов к государственной тайне осуществляется в порядке, устанавливаемом Правительством Российской Федерации.

Допуск должностных лиц и граждан к государственной тайне предусматривает:

- принятие на себя обязательств перед государством по нераспространению доверенных им сведений, составляющих государственную тайну;
- согласие на частичные, временные ограничения их прав в соответствии со статьей 24 настоящего Закона;
- письменное согласие на проведение в отношении их полномочными органами проверочных мероприятий;
- определение видов, размеров и порядка предоставления социальных гарантий, предусмотренных настоящим Законом;
- ознакомление с нормами законодательства Российской Федерации о государственной тайне, предусматривающими ответственность за его нарушение;
- принятие решения руководителем органа государственной власти, предприятия, учреждения или организации о допуске оформляемого лица к сведениям, составляющим государственную тайну.

Объем проверочных мероприятий зависит от степени секретности сведений, к которым будет допускаться оформляемое лицо. Проверочные мероприятия осуществляются в соответствии с законодательством Российской Федерации. Целью проведения проверочных мероприятий является выявление оснований, предусмотренных статьей 22 настоящего Закона.

Для должностных лиц и граждан, допущенных к государственной тайне на постоянной основе, устанавливаются следующие социальные гарантии:

- процентные надбавки к заработной плате в зависимости от степени секретности сведений, к которым они имеют доступ;
- преимущественное право при прочих равных условиях на оставление на работе при проведении органами государственной власти, предприятиями, учреждениями и организациями организационных и (или) штатных мероприятий.

Для сотрудников структурных подразделений по защите государственной тайны дополнительно к социальным гарантиям, установленным для должностных лиц и граждан, допущенных к государственной тайне на постоянной основе, устанавливается процентная надбавка к заработной плате за стаж работы в указанных структурных подразделениях.

Взаимные обязательства администрации и оформляемого лица отражаются в трудовом договоре (контракте). Заключение трудового договора (контракта) до окончания проверки компетентными органами не допускается.

Устанавливается три формы допуска к государственной тайне должностных лиц и граждан, соответствующие трем степеням секретности сведений, составляющих государственную тайну: к сведениям особой важности, совершенно секретным или секретным. Наличие у должностных лиц и граждан допуска к сведениям более высокой степени секретности является основанием для доступа их к сведениям более низкой степени секретности.

Сроки, обстоятельства и порядок переоформления допуска граждан к государственной тайне устанавливаются нормативными документами, утверждаемыми Правительством Российской Федерации.

Порядок допуска должностных лиц и граждан к государственной тайне в условиях объявленного чрезвычайного положения может быть изменен Президентом Российской Федерации.

Статья 21-1. Особый порядок допуска к государственной тайне

Члены Совета Федерации, депутаты Государственной Думы, судьи на период исполнения ими своих полномочий, а также адвокаты, участвующие в качестве защитников в уголовном судопроизводстве по делам, связанным со сведениями, составляющими государственную тайну, допускаются к сведениям, составляющим государственную тайну, без проведения проверочных мероприятий, предусмотренных статьей 21 настоящего Закона.

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.

Сохранность государственной тайны в таких случаях гарантируется путем установления ответственности указанных лиц федеральным законом.

Статья 22. Основания для отказа должностному лицу или гражданину в допуске к государственной тайне

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

- признание его судом недееспособным, ограниченно дееспособным и*ли* рецидивистом, нахождение его под судом или следствием за государственные и иные тяжкие преступления, наличие у него неснятой судимости за эти преступления;
- наличие у него медицинских противопоказаний для работы с использованием сведений, составляющих государственную тайну, согласно перечню, утверждаемому федеральным органом исполнительной власти, уполномоченным в области здравоохранения и социального развития;
- постоянное проживание его самого и (или) его близких родственников за границей и (или) оформление указанными лицами документов для выезда на постоянное жительство в другие государства;
- выявление в результате проверочных мероприятий действий оформляемого лица, создающих угрозу безопасности Российской Федерации;
- уклонение его от проверочных мероприятий и (или) сообщение им заведомо ложных анкетных данных.

Решение об отказе должностному лицу или гражданину в допуске к государственной тайне принимается руководителем органа государственной власти, предприятия, учреждения или организации в индивидуальном порядке с учетом результатов проверочных мероприятий. Гражданин имеет право обжаловать это решение в вышестоящую организацию или в суд.

Статья 23. Условия прекращения допуска должностного лица или гражданина к государственной тайне

Допуск должностного лица или гражданина к государственной тайне может быть прекращен по решению руководителя органа государственной власти, предприятия, учреждения или организации в случаях:

- расторжения с ним трудового договора (контракта) в связи с проведением организационных и (или) штатных мероприятий;
- однократного нарушения им взятых на себя предусмотренных трудовым договором (контрактом) обязательств, связанных с защитой государственной тайны;
- возникновения обстоятельств, являющихся согласно статье 22 настоящего Закона основанием для отказа должностному лицу или гражданину в допуске к государственной тайне.

Прекращение допуска должностного лица или гражданина к государственной тайне является дополнительным основанием для расторжения с ним трудового договора (контракта), если такие условия предусмотрены в трудовом договоре (контракте).

Прекращение допуска к государственной тайне не освобождает должностное лицо или гражданина от взятых ими обязательств по неразглашению сведений, составляющих государственную тайну.

Решение администрации о прекращении допуска должностного лица или гражданина к государственной тайне и расторжении на основании этого с ним трудового договора (контракта) может быть обжаловано в вышестоящую организацию или в суд.

Статья 24. Ограничения прав должностного лица или гражданина, допущенных или ранее допускавшихся к государственной тайне

Должностное лицо или гражданин, допущенные или ранее допускавшиеся к государственной тайне, могут быть временно ограничены в своих правах. Ограничения могут касаться:

- права выезда за границу на срок, оговоренный в трудовом договоре (контракте) при оформлении допуска гражданина к государственной тайне;
- права на распространение сведений, составляющих государственную тайну, и на использование открытий и изобретений, содержащих такие сведения;
- права на неприкосновенность частной жизни при проведении проверочных мероприятий в период оформления допуска к государственной тайне.

Статья 25. Организация доступа должностного лица или гражданина к сведениям, составляющим государственную тайну

Организация доступа должностного лица или гражданина к сведениям, составляющим государственную тайну, возлагается на руководителя соответствующего органа государственной власти, предприятия, учреждения или организации, а также на их структурные подразделения по защите государственной тайны. Порядок доступа должностного лица или гражданина к сведениям, составляющим государственную тайну, устанавливается нормативными документами, утверждаемыми Правительством Российской Федерации.

Руководители органов государственной власти, предприятий, учреждений и организаций несут персональную ответственность за создание таких условий, при которых должностное лицо или гражданин знакомятся только с теми сведениями, составляющими государственную тайну, и в таких объемах, которые необходимы ему для выполнения его должностных (функциональных) обязанностей.

Статья 26. Ответственность за нарушение законодательства Российской Федерации о государственной тайне

Должностные лица и граждане, виновные в нарушении законодательства Российской Федерации о государственной тайне, несут уголовную, административную, гражданско-правовую или дисциплинарную ответственность в соответствии с действующим законодательством.

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

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

Статья 27. Допуск предприятий, учреждений и организаций к проведению работ, связанных с использованием сведений, составляющих государственную тайну

Допуск предприятий, учреждений и организаций к проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны, осуществляется путем получения ими в порядке, устанавливаемом Правительством Российской Федерации, лицензий на проведение работ со сведениями соответствующей степени секретности.

Лицензия на проведение указанных работ выдается на основании результатов специальной экспертизы предприятия, учреждения и организации и государственной аттестации их руководителей, ответственных за защиту сведений, составляющих государственную тайну, расходы по проведению которых относятся на счет предприятия, учреждения, организации, получающих лицензию.

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

- выполнение требований нормативных документов, утверждаемых Правительством Российской Федерации, по обеспечению защиты сведений, составляющих государственную тайну, в процессе выполнения работ, связанных с использованием указанных сведений;
- наличие в их структуре подразделений по защите государственной тайны и специально подготовленных сотрудников для работы, по защите информации, количество и уровень квалификации которых достаточны для обеспечения защиты государственной тайны;
- наличие у них сертифицированных средств защиты информации.

Статья 28. Порядок сертификации средств защиты информации

Средства защиты информации должны иметь сертификат, удостоверяющий их соответствие требованиям по защите сведений соответствующей степени секретности.

Организация сертификации средств защиты информации возлагается на федеральный орган исполнительной власти, уполномоченный в области противодействия техническим разведкам и технической защиты информации, федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности, и федеральный орган исполнительной власти, уполномоченный в области обороны, в соответствии с функциями, возложенными на них законодательством Российской Федерации. Сертификация осуществляется на основании требований государственных стандартов Российской Федерации и иных нормативных документов, утверждаемых Правительством Российской Федерации.

Координация работ по организации сертификации средств защиты информации возлагается на межведомственную комиссию по защите государственной тайны.

Раздел VII Финансирование мероприятий по защите государственной тайны

Статья 29. Финансирование мероприятий по защите государственной тайны

Финансирование деятельности органов государственной власти, бюджетных предприятий, учреждений и организаций и их структурных подразделений по защите государственной тайны, а также социальных гарантий, предусмотренных настоящим Законом, осуществляется за счет средств федерального бюджета, средств бюджетов субъектов Российской Федерации и средств местных бюджетов, а остальных предприятий, учреждений и организаций – за счет средств, получаемых от их основной деятельности при выполнении работ, связанных с использованием сведений, составляющих государственную тайну.

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

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

Раздел VIII Контроль и надзор за обеспечением защиты государственной тайны

Статья 30. Контроль за обеспечением защиты государственной тайны

Контроль за обеспечением защиты государственной тайны осуществляют Президент Российской Федерации, Правительство Российской Федерации в пределах полномочий, определяемых Конституцией Российской Федерации, федеральными конституционными законами и федеральными законами.

Статья 31. Межведомственный и ведомственный контроль

Межведомственный контроль за обеспечением защиты государственной тайны в органах государственной власти, на предприятиях, в учреждениях и организациях осуществляют федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности, федеральный орган исполнительной власти, уполномоченный в области обороны, федеральный орган исполнительной власти, уполномоченный в области внешней разведки, федеральный орган исполнительной власти, уполномоченный в области противодействия техническим разведкам и технической защиты информации, и их территориальные органы, на которые эта функция возложена законодательством Российской Федерации.

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

Контроль за обеспечением защиты государственной тайны в Администрации Президента Российской Федерации, в аппаратах палат Федерального Собрания, Правительства Российской Федерации организуется их руководителями.

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

Статья 32. Прокурорский надзор

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

Доступ лиц, осуществляющих прокурорский надзор, к сведениям, составляющим государственную тайну, осуществляется в соответствии со статьей 25 настоящего Закона.

Президент Российской Федерации

Б.Ельцин

Москва, Дом Советов России

21 июля 1993 г.
№ 5485-I

Приложение Б

Федеральный закон от 29 июля 2004 г. N 98-ФЗ «О коммерческой тайне»

Принят
Государственной Думой
9 июля 2004 года

Одобрен
Советом Федерации
15 июля 2004 года

(в ред. Федеральных законов от 02.02.2006 N 19-ФЗ,
от 18.12.2006 N 231-ФЗ, от 24.07.2007 N 214-ФЗ,
от 11.07.2011 N 200-ФЗ, от 12.03.2014 N 35-ФЗ)

Статья 1. Цели и сфера действия настоящего Федерального закона

1. Настоящий Федеральный закон регулирует отношения, связанные с установлением, изменением и прекращением режима коммерческой тайны в отношении информации, которая имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам.

2. Положения настоящего Федерального закона распространяются на информацию, составляющую коммерческую тайну, независимо от вида носителя, на котором она зафиксирована.

3. Положения настоящего Федерального закона не распространяются на сведения, отнесенные в установленном порядке к государственной тайне, в отношении которой применяются положения законодательства Российской Федерации о государственной тайне.

Статья 3. Основные понятия, используемые в настоящем Федеральном законе

Для целей настоящего Федерального закона используются следующие основные понятия:

1) коммерческая тайна – режим конфиденциальности информации, позволяющий ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду;

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

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 об-

ладателя 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 коммерческую 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.

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 травматизма 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 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 6.1. Права обладателя информации, составляющей коммерческую тайну

1. Права обладателя информации, составляющей коммерческую тайну, возникают с момента установления им в отношении этой информации режима коммерческой тайны в соответствии со статьей 10 настоящего Федерального закона.

2. Обладатель информации, составляющей коммерческую тайну, имеет право:

1) устанавливать, изменять, отменять в письменной форме режим коммерческой тайны в соответствии с настоящим Федеральным законом и гражданско-правовым договором;

2) использовать информацию, составляющую коммерческую тайну, для собственных нужд в порядке, не противоречащем законодательству Российской Федерации;

3) разрешать или запрещать доступ к информации, составляющей коммерческую тайну, определять порядок и условия доступа к этой информации;

4) требовать от юридических лиц, физических лиц, получивших доступ к информации, составляющей коммерческую тайну, органов государственной власти, иных государственных органов, органов местного самоуправления, которым предоставлена информация, составляющая коммерческую тайну, соблюдения обязанностей по охране ее конфиденциальности;

5) требовать от лиц, получивших доступ к информации, составляющей коммерческую тайну, в результате действий, совершенных случайно или по ошибке, охраны конфиденциальности этой информации;

6) защищать в установленном законом порядке свои права в случае разглашения, незаконного получения или незаконного использования третьими лицами информации, составляющей коммерческую тайну, в том числе требовать возмещения убытков, причиненных в связи с нарушением его прав.

Статья 10. Охрана конфиденциальности информации

1. Меры по охране конфиденциальности информации, принимаемые ее обладателем, должны включать в себя:

1) определение перечня информации, составляющей коммерческую тайну;

2) ограничение доступа к информации, составляющей коммерческую тайну, путем установления порядка обращения с этой информацией и контроля за соблюдением такого порядка;

3) учет лиц, получивших доступ к информации, составляющей коммерческую тайну, и (или) лиц, которым такая информация была предоставлена или передана;

4) регулирование отношений по использованию информации, составляющей коммерческую тайну, работниками на основании трудовых договоров и контрагентами на основании гражданско-правовых договоров;

5) нанесение на материальные носители, содержащие информацию, составляющую коммерческую тайну, или включение в состав реквизитов документов, содержащих такую информацию, грифа «Коммерческая тайна» с указанием обладателя такой информации (для юридических лиц – полное наименование и место нахождения, для индивидуальных предпринимателей – фамилия, имя, отчество гражданина, являющегося индивидуальным предпринимателем, и место жительства).

2. Режим коммерческой тайны считается установленным после принятия обладателем информации, составляющей коммерческую тайну, мер, указанных в части 1 настоящей статьи.

3. Индивидуальный предприниматель, являющийся обладателем информации, составляющей коммерческую тайну, и не имеющий работников, с которыми заключены трудовые договоры, принимает меры по охране конфиденциальности информации, указанные в части 1 настоящей статьи, за исключением пунктов 1 и 2, а также положений пункта 4, касающихся регулирования трудовых отношений.

4. Наряду с мерами, указанными в части 1 настоящей статьи, обладатель информации, составляющей коммерческую тайну, вправе применять при необходимости средства и методы технической защиты конфиденциальности этой информации, другие не противоречащие законодательству Российской Федерации меры.

5. Меры по охране конфиденциальности информации признаются разумно достаточными, если:

1) исключается доступ к информации, составляющей коммерческую тайну, любых лиц без согласия ее обладателя;

2) обеспечивается возможность использования информации, составляющей коммерческую тайну, работниками и передачи ее контрагентам без нарушения режима коммерческой тайны.

6. Режим коммерческой тайны не может быть использован в целях, противоречащих требованиям защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства.

Статья 11. Охрана конфиденциальности информации, составляющей коммерческую тайну, в рамках трудовых отношений

1. В целях охраны конфиденциальности информации, составляющей коммерческую тайну, работодатель обязан:

1) ознакомить под расписку работника, доступ которого к этой информации, обладателями которой являются работодатель и его контрагенты, необходим для исполнения данным работником своих трудовых обязанностей, с перечнем информации, составляющей коммерческую тайну;

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

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

2. Доступ работника к информации, составляющей коммерческую тайну, осуществляется с его согласия, если это не предусмотрено его трудовыми обязанностями.

3. В целях охраны конфиденциальности информации, составляющей коммерческую тайну, работник обязан:

1) выполнять установленный работодателем режим коммерческой тайны;

2) не разглашать эту информацию, обладателями которой являются работодатель и его контрагенты, и без их согласия не использовать эту информацию в личных целях в течение всего срока действия режима коммерческой тайны, в том числе после прекращения действия трудового договора;

3) возместить причиненные работодателю убытки, если работник виновен в разглашении информации, составляющей коммерческую тайну и ставшей ему известной в связи с исполнением им трудовых обязанностей;

4) передать работодателю при прекращении или расторжении трудового договора материальные носители информации, имеющиеся в пользовании работника и содержащие информацию, составляющую коммерческую тайну.

4. Работодатель вправе потребовать возмещения убытков, причиненных ему разглашением информации, составляющей коммерческую тайну, от лица, получившего доступ к этой информации в связи с исполнением трудовых обязанностей, но прекратившего трудовые отношения с работодателем, если эта информация разглашена в течение срока действия режима коммерческой тайны.

5. Причиненные работником или прекратившим трудовые отношения с работодателем лицом убытки не возмещаются, если разглашение информации, составляющей коммерческую тайну, произошло вследствие несоблюдения работодателем мер по обеспечению режима коммерческой тайны, действий третьих лиц или непреодолимой силы.

6. Трудовым договором с руководителем организации должны предусматриваться его обязанности по обеспечению охраны конфиденциальности составляющей коммерческую тайну информации, обладателем которой являются организация и ее контрагенты, и ответственность за обеспечение охраны конфиденциальности этой информации.

7. Руководитель организации возмещает организации убытки, причиненные его виновными действиями в связи с нарушением законодательства Российской Федерации о

коммерческой тайне. При этом убытки определяются в соответствии с гражданским законодательством.

8. Работник имеет право обжаловать в судебном порядке незаконное установление режима коммерческой тайны в отношении информации, к которой он получил доступ в связи с исполнением трудовых обязанностей.

Статья 13. Охрана конфиденциальности информации при ее предоставлении

1. Органы государственной власти, иные государственные органы, органы местного самоуправления в соответствии с настоящим Федеральным законом и иными федеральными законами обязаны создать условия, обеспечивающие охрану конфиденциальности информации, предоставленной им юридическими лицами или индивидуальными предпринимателями.

2. Должностные лица органов государственной власти, иных государственных органов, органов местного самоуправления, государственные или муниципальные служащие указанных органов без согласия обладателя информации, составляющей коммерческую тайну, не вправе разглашать или передавать другим лицам, органам государственной власти, иным государственным органам, органам местного самоуправления ставшую известной им в силу выполнения должностных (служебных) обязанностей информацию, составляющую коммерческую тайну, за исключением случаев, предусмотренных настоящим Федеральным законом, а также не вправе использовать эту информацию в корыстных или иных личных целях.

3. В случае нарушения конфиденциальности информации должностными лицами органов государственной власти, иных государственных органов, органов местного самоуправления, государственными и муниципальными служащими указанных органов эти лица несут ответственность в соответствии с законодательством Российской Федерации.

Статья 14. Ответственность за нарушение настоящего Федерального закона

1. Нарушение настоящего Федерального закона влечет за собой дисциплинарную, гражданско-правовую, административную или уголовную ответственность в соответствии с законодательством Российской Федерации.

2. Работник, который в связи с исполнением трудовых обязанностей получил доступ к информации, составляющей коммерческую тайну, обладателями которой являются работодатель и его контрагенты, в случае умышленного или неосторожного разглашения этой информации при отсутствии в действиях такого работника состава преступления несет дисциплинарную ответственность в соответствии с законодательством Российской Федерации.

3. Органы государственной власти, иные государственные органы, органы местного самоуправления, получившие доступ к информации, составляющей коммерческую тайну, несут перед обладателем информации, составляющей коммерческую тайну, гражданско-правовую ответственность за разглашение или незаконное использование этой информации их должностными лицами, государственными или муниципальными служащими указанных органов, которым она стала известна в связи с выполнением ими должностных (служебных) обязанностей.

4. Лицо, которое использовало информацию, составляющую коммерческую тайну, и не имело достаточных оснований считать использование данной информации незаконным, в том числе получило доступ к ней в результате случайности или ошибки, не может в соответствии с настоящим Федеральным законом быть привлечено к ответственности.

5. По требованию обладателя информации, составляющей коммерческую тайну, лицо, указанное в части 4 настоящей статьи, обязано принять меры по охране конфиденциальности информации. При отказе такого лица принять указанные меры обладатель информации, составляющей коммерческую тайну, вправе требовать в судебном порядке защиты своих прав.

Статья 15. Ответственность за непредоставление органам государственной власти, иным государственным органам, органам местного самоуправления информации, составляющей коммерческую тайну

Невыполнение обладателем информации, составляющей коммерческую тайну, законных требований органов государственной власти, иных государственных органов, органов местного самоуправления о предоставлении им информации, составляющей коммерческую тайну, а равно воспрепятствование получению должностными лицами этих органов указанной информации влечет за собой ответственность в соответствии с законодательством Российской Федерации.

Статья 16. Переходные положения

Грифы, нанесенные до вступления в силу настоящего Федерального закона на материальные носители и указывающие на содержание в них информации, составляющей коммерческую тайну, сохраняют свое действие при условии, если меры по охране конфиденциальности указанной информации будут приведены в соответствие с требованиями настоящего Федерального закона.

Президент
Российской Федерации
В.ПУТИН
Москва, Кремль
29 июля 2004 года
N 98-ФЗ

Приложение В

Российская федерация федеральный закон 152-фз
«О персональных данных»

27 июля 2006 года

Принят
Государственной Думой
8 июля 2006 года

Одобрен
Советом Федерации
14 июля 2006 года

Список изменяющих документов
(в ред. Федеральных законов от 25.11.2009 N 266-ФЗ,
от 27.12.2009 N 363-ФЗ, от 28.06.2010 N 123-ФЗ,
от 27.07.2010 N 204-ФЗ, от 27.07.2010 N 227-ФЗ,
от 29.11.2010 N 313-ФЗ от 23.12.2010 N 359-ФЗ,
от 04.06.2011 N 123-ФЗ, от 25.07.2011 N 261-ФЗ,
от 05.04.2013 N 43-ФЗ, от 23.07.2013 N 205-ФЗ,
от 21.12.2013 N 363-ФЗ, от 04.06.2014 N 142-ФЗ,
от 21.07.2014 N 216-ФЗ, от 21.07.2014 N 242-ФЗ,
от 03.07.2016 N 231-ФЗ)

Глава 1. ОБЩИЕ ПОЛОЖЕНИЯ

Статья 1. Сфера действия настоящего Федерального закона

1. Настоящим Федеральным законом регулируются отношения, связанные с обработкой персональных данных, осуществляемой федеральными органами государственной власти, органами государственной власти субъектов Российской Федерации, иными государственными органами (далее – государственные органы), органами местного самоуправления, иными муниципальными органами (далее – муниципальные органы), юридическими лицами и физическими лицами с использованием средств автоматизации, в том числе в информационно-телекоммуникационных сетях, или без использования таких средств, если обработка персональных данных без использования таких средств соответствует характеру действий (операций), совершаемых с персональными данными с использованием средств автоматизации, то есть позволяет осуществлять в соответствии с заданным алгоритмом поиск персональных данных, зафиксированных на материальном носителе и содержащихся в картотеках или иных систематизированных собраниях персональных данных, и (или) доступ к таким персональным данным.

2. Действие настоящего Федерального закона не распространяется на отношения, возникающие при:

1) обработке персональных данных физическими лицами исключительно для личных и семейных нужд, если при этом не нарушаются права субъектов персональных данных;

2) организации хранения, комплектования, учета и использования содержащих персональные данные документов Архивного фонда Российской Федерации и других архивных документов в соответствии с законодательством об архивном деле в Российской Федерации;

3) обработке персональных данных, отнесенных в установленном порядке к сведениям, составляющим государственную тайну;

4) предоставлении уполномоченными органами информации о деятельности судов в Российской Федерации в соответствии с Федеральным законом от 22 декабря 2008 года N 262-ФЗ «Об обеспечении доступа к информации о деятельности судов в Российской Федерации».

Статья 2. Цель настоящего Федерального закона

Целью настоящего Федерального закона является обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну.

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 прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);

2) оператор – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными;

3) обработка персональных данных – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных;

4) автоматизированная обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники;

5) распространение персональных данных – действия, направленные на раскрытие персональных данных неопределенному кругу лиц;

6) предоставление персональных данных – действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;

7) блокирование персональных данных – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);

8) уничтожение персональных данных – действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных;

9) обезличивание персональных данных – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;

10) информационная система персональных данных – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;

11) трансграничная передача персональных данных – передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

Статья 4. Законодательство Российской Федерации в области персональных данных

1. Законодательство Российской Федерации в области персональных данных осно-

вывается на Конституции Российской Федерации и международных договорах Российской Федерации и состоит из настоящего Федерального закона и других определяющих случаи и особенности обработки персональных данных федеральных законов.

2. На основании и во исполнение федеральных законов государственные органы, Банк России, органы местного самоуправления в пределах своих полномочий могут принимать нормативные правовые акты, нормативные акты, правовые акты (далее - нормативные правовые акты) по отдельным вопросам, касающимся обработки персональных данных. Такие акты не могут содержать положения, ограничивающие права субъектов персональных данных, устанавливающие не предусмотренные федеральными законами ограничения деятельности операторов или возлагающие на операторов не предусмотренные федеральными законами обязанности, и подлежат официальному опубликованию.

3. Особенности обработки персональных данных, осуществляемой без использования средств автоматизации, могут быть установлены федеральными законами и иными нормативными правовыми актами Российской Федерации с учетом положений настоящего Федерального закона.

4. Если международным договором Российской Федерации установлены иные правила, чем те, которые предусмотрены настоящим Федеральным законом, применяются правила международного договора.

Глава 2. ПРИНЦИПЫ И УСЛОВИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Статья 5. Принципы обработки персональных данных

1. Обработка персональных данных должна осуществляться на законной и справедливой основе.

2. Обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных.

3. Не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой.

4. Обработке подлежат только персональные данные, которые отвечают целям их обработки.

5. Содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки. Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки.

6. При обработке персональных данных должны быть обеспечены точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных. Оператор должен принимать необходимые меры либо обеспечивать их принятие по удалению или уточнению неполных или неточных данных.

7. Хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных. Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

Статья 6. Условия обработки персональных данных

1. Обработка персональных данных должна осуществляться с соблюдением принципов и правил, предусмотренных настоящим Федеральным законом. Обработка персональных данных допускается в следующих случаях:

1) обработка персональных данных осуществляется с согласия субъекта персональных данных на обработку его персональных данных;

2) обработка персональных данных необходима для достижения целей, предусмотренных международным договором Российской Федерации или законом, для осуществления и выполнения возложенных законодательством Российской Федерации на оператора функций, полномочий и обязанностей;

3) обработка персональных данных необходима для осуществления правосудия, исполнения судебного акта, акта другого органа или должностного лица, подлежащих исполнению в соответствии с законодательством Российской Федерации об исполнительном производстве (далее – исполнение судебного акта);

4) обработка персональных данных необходима для исполнения полномочий федеральных органов исполнительной власти, органов государственных внебюджетных фондов, исполнительных органов государственной власти субъектов Российской Федерации, органов местного самоуправления и функций организаций, участвующих в предоставлении соответственно государственных и муниципальных услуг, предусмотренных Федеральным законом от 27 июля 2010 года N 210-ФЗ «Об организации предоставления государственных и муниципальных услуг», включая регистрацию субъекта персональных данных на едином портале государственных и муниципальных услуг и (или) региональных порталах государственных и муниципальных услуг;

5) обработка персональных данных необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных, а также для заключения договора по инициативе субъекта персональных данных или договора, по которому субъект персональных данных будет являться выгодоприобретателем или поручителем;

6) обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно;

7) обработка персональных данных необходима для осуществления прав и законных интересов оператора или третьих лиц, в том числе в случаях, предусмотренных Федеральным законом «О защите прав и законных интересов физических лиц при осуществлении деятельности по возврату просроченной задолженности и о внесении изменений в Федеральный закон «О микрофинансовой деятельности и микрофинансовых организациях», либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта персональных данных;

8) обработка персональных данных необходима для осуществления профессиональной деятельности журналиста и (или) законной деятельности средства массовой информации либо научной, литературной или иной творческой деятельности при условии, что при этом не нарушаются права и законные интересы субъекта персональных данных;

9) обработка персональных данных осуществляется в статистических или иных исследовательских целях, за исключением целей, указанных в статье 15 настоящего Федерального закона, при условии обязательного обезличивания персональных данных;

10) осуществляется обработка персональных данных, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных либо по его просьбе (далее – персональные данные, сделанные общедоступными субъектом персональных данных);

11) осуществляется обработка персональных данных, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральным законом.

2. Особенности обработки специальных категорий персональных данных, а также биометрических персональных данных устанавливаются соответственно статьями 10 и 11 настоящего Федерального закона.

3. Оператор вправе поручить обработку персональных данных другому лицу с согласия субъекта персональных данных, если иное не предусмотрено федеральным законом, на основании заключаемого с этим лицом договора, в том числе государственного или муниципального контракта, либо путем принятия государственным или муниципальным органом соответствующего акта (далее – поручение оператора). Лицо, осуществляющее обработку персональных данных по поручению оператора, обязано соблюдать принципы и правила обработки персональных данных, предусмотренные настоящим Федеральным законом. В поручении оператора должны быть определены перечень действий (операций) с персональными данными, которые будут совершаться лицом, осуществляющим обработку персональных данных, и цели обработки, должна быть установлена обязанность такого лица соблюдать конфиденциальность персональных данных и обеспечивать безопасность персональных данных при их обработке, а также должны быть указаны требования к защите обрабатываемых персональных данных в соответствии со статьей 19 настоящего Федерального закона.

4. Лицо, осуществляющее обработку персональных данных по поручению оператора, не обязано получать согласие субъекта персональных данных на обработку его персональных данных.

5. В случае, если оператор поручает обработку персональных данных другому лицу, ответственность перед субъектом персональных данных за действия указанного лица несет оператор. Лицо, осуществляющее обработку персональных данных по поручению оператора, несет ответственность перед оператором.

Статья 7. Конфиденциальность персональных данных

Операторы и иные лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

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, сообщаемые субъектом персональных данных.

2. Сведения о субъекте персональных данных должны быть в любое время исключены из общедоступных источников персональных данных по требованию субъекта персональных данных либо по решению суда или иных уполномоченных государственных органов.

Статья 9. Согласие субъекта персональных данных на обработку его персональных данных

1. Субъект персональных данных принимает решение о предоставлении его персональных данных и дает согласие на их обработку свободно, своей волей и в своем интересе. Согласие на обработку персональных данных должно быть конкретным, информированным и сознательным. Согласие на обработку персональных данных может быть дано субъектом персональных данных или его представителем в любой позволяющей подтвердить факт его получения форме, если иное не установлено федеральным законом. В случае получения согласия на обработку персональных данных от

представителя субъекта персональных данных полномочия данного представителя на дачу согласия от имени субъекта персональных данных проверяются оператором.

2. Согласие на обработку персональных данных может быть отозвано субъектом персональных данных. В случае отзыва субъектом персональных данных согласия на обработку персональных данных оператор вправе продолжить обработку персональных данных без согласия субъекта персональных данных при наличии оснований, указанных в пунктах 2–11 части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11 настоящего Федерального закона.

3. Обязанность предоставить доказательство получения согласия субъекта персональных данных на обработку его персональных данных или доказательство наличия оснований, указанных в пунктах 2–11 части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11 настоящего Федерального закона, возлагается на оператора.

4. В случаях, предусмотренных федеральным законом, обработка персональных данных осуществляется только с согласия в письменной форме субъекта персональных данных. Равнозначным содержащему собственноручную подпись субъекта персональных данных согласию в письменной форме на бумажном носителе признается согласие в форме электронного документа, подписанного в соответствии с федеральным законом электронной подписью. Согласие в письменной форме субъекта персональных данных на обработку его персональных данных должно включать в себя, в частности:

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

2) фамилию, имя, отчество, адрес представителя субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе, реквизиты доверенности или иного документа, подтверждающего полномочия этого представителя (при получении согласия от представителя субъекта персональных данных);

3) наименование или фамилию, имя, отчество и адрес оператора, получающего согласие субъекта персональных данных;

4) цель обработки персональных данных;

5) перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;

6) наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка будет поручена такому лицу;

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

8) срок, в течение которого действует согласие субъекта персональных данных, а также способ его отзыва, если иное не установлено федеральным законом;

9) подпись субъекта персональных данных.

5. Порядок получения в форме электронного документа согласия субъекта персональных данных на обработку его персональных данных в целях предоставления государственных и муниципальных услуг, а также услуг, которые являются необходимыми и обязательными для предоставления государственных и муниципальных услуг, устанавливается Правительством Российской Федерации.

6. В случае недееспособности субъекта персональных данных согласие на обработку его персональных данных дает законный представитель субъекта персональных данных.

7. В случае смерти субъекта персональных данных согласие на обработку его персональных данных дают наследники субъекта персональных данных, если такое согласие не было дано субъектом персональных данных при его жизни.

8. Персональные данные могут быть получены оператором от лица, не являющегося субъектом персональных данных, при условии предоставления оператору подтверждения наличия оснований, указанных в пунктах 2–11 части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11 настоящего Федерального закона.

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 сделаны общедоступными субъектом персональных данных;

2.1) обработка персональных данных необходима в связи с реализацией международных договоров Российской Федерации о реадмиссии;

2.2) обработка персональных данных осуществляется в соответствии с Федеральным законом от 25 января 2002 года N 8-ФЗ «О Всероссийской переписи населения»;

2.3) обработка персональных данных осуществляется в соответствии с законодательством о государственной социальной помощи, трудовым законодательством, пенсионным законодательством Российской Федерации;

3) обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных либо жизни, здоровья или иных жизненно важных интересов других лиц и получение согласия субъекта персональных данных невозможно;

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 медицинской 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 для установления или осуществления прав субъекта персональных данных или третьих лиц, а равно и в связи с осуществлением правосудия;

7) обработка персональных данных осуществляется в соответствии с законодательством Российской Федерации об обороне, о безопасности, о противодействии терроризму, о транспортной безопасности, о противодействии коррупции, об оперативно-разыскной деятельности, об исполнительном производстве, уголовно-исполнительным законодательством Российской Федерации;

7.1) обработка полученных в установленных законодательством Российской Федерации случаях персональных данных осуществляется органами прокуратуры в связи с осуществлением ими прокурорского надзора;

8) обработка персональных данных осуществляется в соответствии с законодательством об обязательных видах страхования, со страховым законодательством;

9) обработка персональных данных осуществляется в случаях, предусмотренных

законодательством Российской Федерации, государственными органами, муниципальными органами или организациями в целях устройства детей, оставшихся без попечения родителей, на воспитание в семьи граждан;

10) обработка персональных данных осуществляется в соответствии с законодательством Российской Федерации о гражданстве 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, если иное не установлено федеральным законом.

Статья 11. Биометрические персональные данные

1. Сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность (биометрические персональные данные) и которые используются оператором для установления личности субъекта персональных данных, 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 реализацией международных договоров Российской Федерации о реадмиссии, в связи с осуществлением правосудия и исполнением судебных актов, а также в случаях, предусмотренных законодательством Российской Федерации об обороне, о безопасности, о противодействии терроризму, о транспортной безопасности, о противодействии коррупции, об оперативно-разыскной деятельности, о государственной службе, уголовно-исполнительным законодательством Российской Федерации, законодательством Российской Федерации о порядке выезда из Российской Федерации и въезда в Российскую Федерацию, о гражданстве Российской Федерации.

Статья 12. Трансграничная передача персональных данных

1. Трансграничная передача персональных данных на территории иностранных государств, являющихся сторонами Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных, а также иных иностранных государств, обеспечивающих адекватную защиту прав субъектов персональных данных, осуществляется в соответствии с настоящим Федеральным законом и может быть запрещена или ограничена в целях защиты основ конституционного строя Российской Федерации, нравственности, здоровья, прав и законных интересов граждан, обеспечения обороны страны и безопасности государства.

2. Уполномоченный орган по защите прав субъектов персональных данных утверждает перечень иностранных государств, не являющихся сторонами Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных и обеспечивающих адекватную защиту прав субъектов персональных данных. Государство, не являющееся стороной Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных, может быть включено в перечень иностранных государств, обеспечивающих адекватную защиту прав субъектов персональных данных, при условии соответствия положениям указанной Конвенции действующих в соответствующем государстве норм права и применяемых мер безопасности персональных данных.

3. Оператор обязан убедиться в том, что иностранным государством, на территорию которого осуществляется передача персональных данных, обеспечивается адекватная защита прав субъектов персональных данных, до начала осуществления трансграничной передачи персональных данных.

4. Трансграничная передача персональных данных на территории иностранных государств, не обеспечивающих адекватной защиты прав субъектов персональных данных, может осуществляться в случаях:

1) наличия согласия в письменной форме субъекта персональных данных на трансграничную передачу его персональных данных;

2) предусмотренных международными договорами Российской Федерации;

3) предусмотренных федеральными законами, если это необходимо в целях защиты основ конституционного строя Российской Федерации, обеспечения обороны страны и безопасности государства, а также обеспечения безопасности устойчивого и безопасного функционирования транспортного комплекса, защиты интересов личности, общества и государства в сфере транспортного комплекса от актов незаконного вмешательства;

4) исполнения договора, стороной которого является субъект персональных данных;

5) защиты жизни, здоровья, иных жизненно важных интересов субъекта персональных данных или других лиц при невозможности получения согласия в письменной форме субъекта персональных данных.

Статья 13. Особенности обработки персональных данных в государственных или муниципальных информационных системах персональных данных

1. Государственные органы, муниципальные органы создают в пределах своих полномочий, установленных в соответствии с федеральными законами, государственные или муниципальные информационные системы персональных данных.

2. Федеральными законами могут быть установлены особенности учета персональных данных в государственных и муниципальных информационных системах персональных данных, в том числе использование различных способов обозначения принадлежности персональных данных, содержащихся в соответствующей государственной или муниципальной информационной системе персональных данных, конкретному субъекту персональных данных.

3. Права и свободы человека и гражданина не могут быть ограничены по мотивам, связанным с использованием различных способов обработки персональных данных или обозначения принадлежности персональных данных, содержащихся в государственных или муниципальных информационных системах персональных данных, конкретному субъекту персональных данных. Не допускается использование оскорбляющих чувства граждан или унижающих человеческое достоинство способов обозначения принадлежности персональных данных, содержащихся в государственных или муниципальных информационных системах персональных данных, конкретному субъекту персональных данных.

4. В целях обеспечения реализации прав субъектов персональных данных в связи с обработкой их персональных данных в государственных или муниципальных информационных системах персональных данных может быть создан государственный регистр населения, правовой статус которого и порядок работы с которым устанавливаются федеральным законом.

Глава 3. ПРАВА СУБЪЕКТА ПЕРСОНАЛЬНЫХ ДАННЫХ

Статья 14. Право субъекта персональных данных на доступ к его персональным данным

1. Субъект персональных данных имеет право на получение сведений, указанных в

части 7 настоящей статьи, за исключением случаев, предусмотренных частью 8 настоящей статьи. Субъект персональных данных вправе требовать от оператора уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

2. Сведения, указанные в части 7 настоящей статьи, должны быть предоставлены субъекту персональных данных оператором в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных, за исключением случаев, если имеются законные основания для раскрытия таких персональных данных.

3. Сведения, указанные в части 7 настоящей статьи, предоставляются субъекту персональных данных или его представителю оператором при обращении либо при получении запроса субъекта персональных данных или его представителя. Запрос должен содержать номер основного документа, удостоверяющего личность субъекта персональных данных или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе, сведения, подтверждающие участие субъекта персональных данных в отношениях с оператором (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных оператором, подпись субъекта персональных данных или его представителя. Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации.

4. В случае, если сведения, указанные в части 7 настоящей статьи, а также обрабатываемые персональные данные были предоставлены для ознакомления субъекту персональных данных по его запросу, субъект персональных данных вправе обратиться повторно к оператору или направить ему повторный запрос в целях получения сведений, указанных в части 7 настоящей статьи, и ознакомления с такими персональными данными не ранее чем через тридцать дней после первоначального обращения или направления первоначального запроса, если более короткий срок не установлен федеральным законом, принятым в соответствии с ним нормативным правовым актом или договором, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных.

5. Субъект персональных данных вправе обратиться повторно к оператору или направить ему повторный запрос в целях получения сведений, указанных в части 7 настоящей статьи, а также в целях ознакомления с обрабатываемыми персональными данными до истечения срока, указанного в части 4 настоящей статьи, в случае, если такие сведения и (или) обрабатываемые персональные данные не были предоставлены ему для ознакомления в полном объеме по результатам рассмотрения первоначального обращения. Повторный запрос наряду со сведениями, указанными в части 3 настоящей статьи, должен содержать обоснование направления повторного запроса.

6. Оператор вправе отказать субъекту персональных данных в выполнении повторного запроса, не соответствующего условиям, предусмотренным частями 4 и 5 настоящей статьи. Такой отказ должен быть мотивированным. Обязанность представления доказательств обоснованности отказа в выполнении повторного запроса лежит на операторе.

7. Субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных, в том числе содержащей:

1) подтверждение факта обработки персональных данных оператором;

2) правовые основания и цели обработки персональных данных;

3) цели и применяемые оператором способы обработки персональных данных;

4) наименование и место нахождения оператора, сведения о лицах (за исключением работников оператора), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с оператором или на основании федерального закона;

5) обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;

6) сроки обработки персональных данных, в том числе сроки их хранения;

7) порядок осуществления субъектом персональных данных прав, предусмотренных настоящим Федеральным законом;

8) информацию об осуществленной или о предполагаемой трансграничной передаче данных;

9) наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка поручена или будет поручена такому лицу;

10) иные сведения, предусмотренные настоящим Федеральным законом или другими федеральными законами.

8. Право субъекта персональных данных на доступ к его персональным данным может быть ограничено в соответствии с федеральными законами, в том числе если:

1) обработка персональных данных, включая персональные данные, полученные в результате оперативно-разыскной, 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) обработка персональных данных осуществляется в соответствии с законодательством о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма;

4) доступ субъекта персональных данных к его персональным данным нарушает права и законные интересы третьих лиц;

5) обработка персональных данных осуществляется в случаях, предусмотренных законодательством Российской Федерации о транспортной безопасности, в целях обеспечения устойчивого и безопасного функционирования транспортного комплекса, защиты интересов личности, общества и государства в сфере транспортного комплекса от актов незаконного вмешательства.

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 тридцати дней со дня его получения и уведомить субъекта персональных данных о результатах рассмотрения такого возражения.

Статья 17. Право на обжалование действий или бездействия оператора

1. Если субъект персональных данных считает, что оператор осуществляет обработку его персональных данных с нарушением требований настоящего Федерального закона или иным образом нарушает его права и свободы, субъект персональных данных вправе обжаловать действия или бездействие оператора в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке.

2. Субъект персональных данных имеет право на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.

Глава 4. ОБЯЗАННОСТИ ОПЕРАТОРА

Статья 18. Обязанности оператора при сборе персональных данных

1. При сборе персональных данных оператор обязан предоставить субъекту персональных данных по его просьбе информацию, предусмотренную частью 7 статьи 14 настоящего Федерального закона.

2. Если предоставление персональных данных является обязательным в соответствии с федеральным законом, оператор обязан разъяснить субъекту персональных данных юридические последствия отказа предоставить его персональные данные.

3. Если персональные данные получены не от субъекта персональных данных, оператор, за исключением случаев, предусмотренных частью 4 настоящей статьи, до начала обработки таких персональных данных обязан предоставить субъекту персональных данных следующую информацию:

1) наименование либо фамилия, имя, отчество и адрес оператора или его представителя;

2) цель обработки персональных данных и ее правовое основание;

3) предполагаемые пользователи персональных данных;

4) установленные настоящим Федеральным законом права субъекта персональных данных;

5) источник получения персональных данных.

4. Оператор освобождается от обязанности предоставить субъекту персональных данных сведения, предусмотренные частью 3 настоящей статьи, в случаях, если:

1) субъект персональных данных уведомлен об осуществлении обработки его персональных данных соответствующим оператором;

2) персональные данные получены оператором на основании федерального закона или в связи с исполнением договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных;

3) персональные данные сделаны общедоступными субъектом персональных данных или получены из общедоступного источника;

4) оператор осуществляет обработку персональных данных для статистических или иных исследовательских целей, для осуществления профессиональной деятельности журналиста либо научной, литературной или иной творческой деятельности, если при этом не нарушаются права и законные интересы субъекта персональных данных;

5) предоставление субъекту персональных данных сведений, предусмотренных частью 3 настоящей статьи, нарушает права и законные интересы третьих лиц.

5. При сборе персональных данных, в том числе посредством информационно-телекоммуникационной сети «Интернет», оператор обязан обеспечить запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации с использованием баз данных, находящихся на территории Российской Федерации, за исключением случаев, указанных в пунктах 2, 3, 4, 8 части 1 статьи 6 настоящего Федерального закона.

Статья 18.1. Меры, направленные на обеспечение выполнения оператором обязанностей, предусмотренных настоящим Федеральным законом

1. Оператор обязан принимать меры, необходимые и достаточные для обеспечения выполнения обязанностей, предусмотренных настоящим Федеральным законом и принятыми в соответствии с ним нормативными правовыми актами. Оператор самостоятельно определяет состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных настоящим Федеральным законом и принятыми в соответствии с ним нормативными правовыми актами, если иное не предусмотрено настоящим Федеральным законом или другими федеральными законами. К таким мерам могут, в частности, относиться:

1) назначение оператором, являющимся юридическим лицом, ответственного за организацию обработки персональных данных;

2) издание оператором, являющимся юридическим лицом, документов, определяющих политику оператора в отношении обработки персональных данных, локальных актов по вопросам обработки персональных данных, а также локальных актов, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений;

3) применение правовых, организационных и технических мер по обеспечению безопасности персональных данных в соответствии со статьей 19 настоящего Федерального закона;

4) осуществление внутреннего контроля и (или) аудита соответствия обработки персональных данных настоящему Федеральному закону и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, политике оператора в отношении обработки персональных данных, локальным актам оператора;

5) оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения настоящего Федерального закона, соотношение указанного вреда и

принимаемых оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных настоящим Федеральным законом;

6) ознакомление работников оператора, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите персональных данных, документами, определяющими политику оператора в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных, и (или) обучение указанных работников.

2. Оператор обязан опубликовать или иным образом обеспечить неограниченный доступ к документу, определяющему его политику в отношении обработки персональных данных, к сведениям о реализуемых требованиях к защите персональных данных. Оператор, осуществляющий сбор персональных данных с использованием информационно-телекоммуникационных сетей, обязан опубликовать в соответствующей информационно-телекоммуникационной сети документ, определяющий его политику в отношении обработки персональных данных, и сведения о реализуемых требованиях к защите персональных данных, а также обеспечить возможность доступа к указанному документу с использованием средств соответствующей информационно-телекоммуникационной сети.

3. Правительство Российской Федерации устанавливает перечень мер, направленных на обеспечение выполнения обязанностей, предусмотренных настоящим Федеральным законом и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами.

4. Оператор обязан представить документы и локальные акты, указанные в части 1 настоящей статьи, и (или) иным образом подтвердить принятие мер, указанных в части 1 настоящей статьи, по запросу уполномоченного органа по защите прав субъектов персональных данных.

Статья 19. Меры по обеспечению безопасности персональных данных при их обработке

1. Оператор при обработке персональных данных обязан принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

2. Обеспечение безопасности персональных данных достигается, в частности:

1) определением угроз безопасности персональных данных при их обработке в информационных системах персональных данных;

2) применением организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных;

3) применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;

4) оценкой эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;

5) учетом машинных носителей персональных данных;

6) обнаружением фактов несанкционированного доступа к персональным данным и принятием мер;

7) восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

8) установлением правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных;

9) контролем за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных.

3. Правительство Российской Федерации с учетом возможного вреда субъекту персональных данных, объема и содержания обрабатываемых персональных данных, вида деятельности, при осуществлении которого обрабатываются персональные данные, актуальности угроз безопасности персональных данных устанавливает:

1) уровни защищенности персональных данных при их обработке в информационных системах персональных данных в зависимости от угроз безопасности этих данных;

2) требования к защите персональных данных при их обработке в информационных системах персональных данных, исполнение которых обеспечивает установленные уровни защищенности персональных данных;

3) требования к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных.

4. Состав и содержание необходимых для выполнения установленных Правительством Российской Федерации в соответствии с частью 3 настоящей статьи требований к защите персональных данных для каждого из уровней защищенности, организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных устанавливаются федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, в пределах их полномочий.

5. Федеральные органы исполнительной власти, осуществляющие функции по выработке государственной политики и нормативно-правовому регулированию в установленной сфере деятельности, органы государственной власти субъектов Российской Федерации, Банк России, органы государственных внебюджетных фондов, иные государственные органы в пределах своих полномочий принимают нормативные правовые акты, в которых определяют угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности, с учетом содержания персональных данных, характера и способов их обработки.

6. Наряду с угрозами безопасности персональных данных, определенных в нормативных правовых актах, принятых в соответствии с частью 5 настоящей статьи, ассоциации, союзы и иные объединения операторов своими решениями вправе определить дополнительные угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении определенных видов деятельности членами таких ассоциаций, союзов и иных объединений операторов, с учетом содержания персональных данных, характера и способов их обработки.

7. Проекты нормативных правовых актов, указанных в части 5 настоящей статьи, подлежат согласованию с федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации. Проекты решений, указанных в части 6 настоящей статьи,

подлежат согласованию с федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, в порядке, установленном Правительством Российской Федерации. Решение федерального органа исполнительной власти, уполномоченного в области обеспечения безопасности, и федерального органа исполнительной власти, уполномоченного в области противодействия техническим разведкам и технической защиты информации, об отказе в согласовании проектов решений, указанных в части 6 настоящей статьи, должно быть мотивированным.

8. Контроль и надзор за выполнением организационных и технических мер по обеспечению безопасности персональных данных, установленных в соответствии с настоящей статьей, при обработке персональных данных в государственных информационных системах персональных данных осуществляются федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, в пределах их полномочий и без права ознакомления с персональными данными, обрабатываемыми в информационных системах персональных данных.

9. Федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности, и федеральный орган исполнительной власти, уполномоченный в области противодействия техническим разведкам и технической защиты информации, решением Правительства Российской Федерации с учетом значимости и содержания обрабатываемых персональных данных могут быть наделены полномочиями по контролю за выполнением организационных и технических мер по обеспечению безопасности персональных данных, установленных в соответствии с настоящей статьей, при их обработке в информационных системах персональных данных, эксплуатируемых при осуществлении определенных видов деятельности и не являющихся государственными информационными системами персональных данных, без права ознакомления с персональными данными, обрабатываемыми в информационных системах персональных данных.

10. Использование и хранение биометрических персональных данных вне информационных систем персональных данных могут осуществляться только на таких материальных носителях информации и с применением такой технологии ее хранения, которые обеспечивают защиту этих данных от неправомерного или случайного доступа к ним, их уничтожения, изменения, блокирования, копирования, предоставления, распространения.

11. Для целей настоящей статьи под угрозами безопасности персональных данных понимается совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия при их обработке в информационной системе персональных данных. Под уровнем защищенности персональных данных понимается комплексный показатель, характеризующий требования, исполнение которых обеспечивает нейтрализацию определенных угроз безопасности персональных данных при их обработке в информационных системах персональных данных.

Статья 20. Обязанности оператора при обращении к нему субъекта персональных данных либо при получении запроса субъекта персональных данных или его представителя, а также уполномоченного органа по защите прав субъектов персональных данных

1. Оператор обязан сообщить в порядке, предусмотренном статьей 14 настоящего Федерального закона, субъекту персональных данных или его представителю инфор-

мацию о наличии персональных данных, относящихся к соответствующему субъекту персональных данных, а также предоставить возможность ознакомления с этими персональными данными при обращении субъекта персональных данных или его представителя либо в течение тридцати дней с даты получения запроса субъекта персональных данных или его представителя.

2. В случае отказа в предоставлении информации о наличии персональных данных о соответствующем субъекте персональных данных или персональных данных субъекту персональных данных или его представителю при их обращении либо при получении запроса субъекта персональных данных или его представителя оператор обязан дать в письменной форме мотивированный ответ, содержащий ссылку на положение части 8 статьи 14 настоящего Федерального закона или иного федерального закона, являющееся основанием для такого отказа, в срок, не превышающий тридцати дней со дня обращения субъекта персональных данных или его представителя либо с даты получения запроса субъекта персональных данных или его представителя.

3. Оператор обязан предоставить безвозмездно субъекту персональных данных или его представителю возможность ознакомления с персональными данными, относящимися к этому субъекту персональных данных. В срок, не превышающий семи рабочих дней со дня предоставления субъектом персональных данных или его представителем сведений, подтверждающих, что персональные данные являются неполными, неточными или неактуальными, оператор обязан внести в них необходимые изменения. В срок, не превышающий семи рабочих дней со дня представления субъектом персональных данных или его представителем сведений, подтверждающих, что такие персональные данные являются незаконно полученными или не являются необходимыми для заявленной цели обработки, оператор обязан уничтожить такие персональные данные. Оператор обязан уведомить субъекта персональных данных или его представителя о внесенных изменениях и предпринятых мерах и принять разумные меры для уведомления третьих лиц, которым персональные данные этого субъекта были переданы.

4. Оператор обязан сообщить в уполномоченный орган по защите прав субъектов персональных данных по запросу этого органа необходимую информацию в течение тридцати дней с даты получения такого запроса.

Статья 21. Обязанности оператора по устранению нарушений законодательства, допущенных при обработке персональных данных, по уточнению, блокированию и уничтожению персональных данных

1. В случае выявления неправомерной обработки персональных данных при обращении субъекта персональных данных или его представителя либо по запросу субъекта персональных данных или его представителя либо уполномоченного органа по защите прав субъектов персональных данных оператор обязан осуществить блокирование неправомерно обрабатываемых персональных данных, относящихся к этому субъекту персональных данных, или обеспечить их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) с момента такого обращения или получения указанного запроса на период проверки. В случае выявления неточных персональных данных при обращении субъекта персональных данных или его представителя либо по их запросу или по запросу уполномоченного органа по защите прав субъектов персональных данных оператор обязан осуществить блокирование персональных данных, относящихся к этому субъекту персональных данных, или обеспечить их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) с момента такого обращения или получения указанного запроса на период проверки, если блокирование персональных данных не нарушает права и законные интересы субъекта персональных данных или третьих лиц.

2. В случае подтверждения факта неточности персональных данных оператор на основании сведений, представленных субъектом персональных данных или его представителем либо уполномоченным органом по защите прав субъектов персональных данных, или иных необходимых документов обязан уточнить персональные данные либо обеспечить их уточнение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) в течение семи рабочих дней со дня представления таких сведений и снять блокирование персональных данных.

3. В случае выявления неправомерной обработки персональных данных, осуществляемой оператором или лицом, действующим по поручению оператора, оператор в срок, не превышающий трех рабочих дней с даты этого выявления, обязан прекратить неправомерную обработку персональных данных или обеспечить прекращение неправомерной обработки персональных данных лицом, действующим по поручению оператора. В случае, если обеспечить правомерность обработки персональных данных невозможно, оператор в срок, не превышающий десяти рабочих дней с даты выявления неправомерной обработки персональных данных, обязан уничтожить такие персональные данные или обеспечить их уничтожение. Об устранении допущенных нарушений или об уничтожении персональных данных оператор обязан уведомить субъекта персональных данных или его представителя, а в случае, если обращение субъекта персональных данных или его представителя либо запрос уполномоченного органа по защите прав субъектов персональных данных были направлены уполномоченным органом по защите прав субъектов персональных данных, также указанный орган.

4. В случае достижения цели обработки персональных данных оператор обязан прекратить обработку персональных данных или обеспечить ее прекращение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) и уничтожить персональные данные или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) в срок, не превышающий тридцати дней с даты достижения цели обработки персональных данных, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между оператором и субъектом персональных данных либо если оператор не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных настоящим Федеральным законом или другими федеральными законами.

5. В случае отзыва субъектом персональных данных согласия на обработку его персональных данных оператор обязан прекратить их обработку или обеспечить прекращение такой обработки (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) и в случае, если сохранение персональных данных более не требуется для целей обработки персональных данных, уничтожить персональные данные или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) в срок, не превышающий тридцати дней с даты поступления указанного отзыва, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между оператором и субъектом персональных данных либо если оператор не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных настоящим Федеральным законом или другими федеральными законами.

6. В случае отсутствия возможности уничтожения персональных данных в течение срока, указанного в частях 3–5 настоящей статьи, оператор осуществляет блокирование таких персональных данных или обеспечивает их блокирование (если обработка персо-

нальных данных осуществляется другим лицом, действующим по поручению оператора) и обеспечивает уничтожение персональных данных в срок не более чем шесть месяцев, если иной срок не установлен федеральными законами.

Статья 22. Уведомление об обработке персональных данных

1. Оператор до начала обработки персональных данных обязан уведомить уполномоченный орган по защите прав субъектов персональных данных о своем намерении осуществлять обработку персональных данных, за исключением случаев, предусмотренных частью 2 настоящей статьи.

2. Оператор вправе осуществлять без уведомления уполномоченного органа по защите прав субъектов персональных данных обработку персональных данных:

1) обрабатываемых в соответствии с трудовым законодательством;

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

3) относящихся к членам (участникам) общественного объединения или религиозной организации и обрабатываемых 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 или раскрываться третьим лицам без согласия в письменной форме субъектов персональных данных;

4) сделанных субъектом персональных данных общедоступными;

5) включающих в себя только фамилии, имена и отчества субъектов персональных данных;

6) необходимых в целях однократного пропуска субъекта персональных данных на территорию, на которой находится оператор, или в иных аналогичных целях;

7) включенных в информационные системы персональных данных, имеющие в соответствии с федеральными законами статус государственных автоматизированных информационных систем, а также в государственные информационные системы персональных данных, созданные в целях защиты безопасности государства и общественного порядка;

8) обрабатываемых без использования средств автоматизации в соответствии с федеральными законами или иными нормативными правовыми актами Российской Федерации, устанавливающими требования к обеспечению безопасности персональных данных при их обработке и к соблюдению прав субъектов персональных данных;

9) обрабатываемых в случаях, предусмотренных законодательством Российской Федерации о транспортной безопасности, в целях обеспечения устойчивого и безопасного функционирования транспортного комплекса, защиты интересов личности, общества и государства в сфере транспортного комплекса от актов незаконного вмешательства.

3. Уведомление, предусмотренное частью 1 настоящей статьи, направляется в виде документа на бумажном носителе или в форме электронного документа и подписывается уполномоченным лицом. Уведомление должно содержать следующие сведения:

1) наименование (фамилия, имя, отчество), адрес оператора;

2) цель обработки персональных данных;

3) категории персональных данных;

4) категории субъектов, персональные данные которых обрабатываются;

5) правовое основание обработки персональных данных;

6) перечень действий с персональными данными, общее описание используемых оператором способов обработки персональных данных;

7) описание мер, предусмотренных статьями 18.1 и 19 настоящего Федерального закона, в том числе сведения о наличии шифровальных (криптографических) средств и наименования этих средств;

7.1) фамилия, имя, отчество физического лица или наименование юридического лица, ответственных за организацию обработки персональных данных, и номера их контактных телефонов, почтовые адреса и адреса электронной почты;

8) дата начала обработки персональных данных;

9) срок или условие прекращения обработки персональных данных;

10) сведения о наличии или об отсутствии трансграничной передачи персональных данных в процессе их обработки;

10.1) сведения о месте нахождения базы данных информации, содержащей персональные данные граждан Российской Федерации;

11) сведения об обеспечении безопасности персональных данных в соответствии с требованиями к защите персональных данных, установленными Правительством Российской Федерации.

4. Уполномоченный орган по защите прав субъектов персональных данных в течение тридцати дней с даты поступления уведомления об обработке персональных данных вносит сведения, указанные в части 3 настоящей статьи, а также сведения о дате направления указанного уведомления в реестр операторов. Сведения, содержащиеся в реестре операторов, за исключением сведений о средствах обеспечения безопасности персональных данных при их обработке, являются общедоступными.

5. На оператора не могут возлагаться расходы в связи с рассмотрением уведомления об обработке персональных данных уполномоченным органом по защите прав субъектов персональных данных, а также в связи с внесением сведений в реестр операторов.

6. В случае предоставления неполных или недостоверных сведений, указанных в части 3 настоящей статьи, уполномоченный орган по защите прав субъектов персональных данных вправе требовать от оператора уточнения предоставленных сведений до их внесения в реестр операторов.

7. В случае изменения сведений, указанных в части 3 настоящей статьи, а также в случае прекращения обработки персональных данных оператор обязан уведомить об этом уполномоченный орган по защите прав субъектов персональных данных в течение десяти рабочих дней с даты возникновения таких изменений или с даты прекращения обработки персональных данных.

Статья 22.1. Лица, ответственные за организацию обработки персональных данных в организациях

1. Оператор, являющийся юридическим лицом, назначает лицо, ответственное за организацию обработки персональных данных.

2. Лицо, ответственное за организацию обработки персональных данных, получает указания непосредственно от исполнительного органа организации, являющейся оператором, и подотчетно ему.

3. Оператор обязан предоставлять лицу, ответственному за организацию обработки персональных данных, сведения, указанные в части 3 статьи 22 настоящего Федерального закона.

4. Лицо, ответственное за организацию обработки персональных данных, в частности, обязано:

1) осуществлять внутренний контроль за соблюдением оператором и его работниками законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных;

2) доводить до сведения работников оператора положения законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных;

3) организовывать прием и обработку обращений и запросов субъектов персональных данных или их представителей и (или) осуществлять контроль за приемом и обработкой таких обращений и запросов.

Глава 5. КОНТРОЛЬ И НАДЗОР ЗА ОБРАБОТКОЙ ПЕРСОНАЛЬНЫХ ДАННЫХ. ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЕ ТРЕБОВАНИЙ НАСТОЯЩЕГО ФЕДЕРАЛЬНОГО ЗАКОНА

Статья 23. Уполномоченный орган по защите прав субъектов персональных данных

1. Уполномоченным органом по защите прав субъектов персональных данных, на который возлагается обеспечение контроля и надзора за соответствием обработки персональных данных требованиям настоящего Федерального закона, является федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере информационных технологий и связи.

2. Уполномоченный орган по защите прав субъектов персональных данных рассматривает обращения субъекта персональных данных о соответствии содержания персональных данных и способов их обработки целям их обработки и принимает соответствующее решение.

3. Уполномоченный орган по защите прав субъектов персональных данных имеет право:

1) запрашивать у физических или юридических лиц информацию, необходимую для реализации своих полномочий, и безвозмездно получать такую информацию;

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

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

3.1) ограничивать доступ к информации, обрабатываемой с нарушением законодательства Российской Федерации в области персональных данных, в порядке, установленном законодательством Российской Федерации;

4) принимать в установленном законодательством Российской Федерации порядке меры по приостановлению или прекращению обработки персональных данных, осуществляемой с нарушением требований настоящего Федерального закона;

5) обращаться в суд с исковыми заявлениями в защиту прав субъектов персональных данных, в том числе в защиту прав неопределенного круга лиц, и представлять интересы субъектов персональных данных в суде;

5.1) направлять в федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности, и федеральный орган исполнительной власти, уполномоченный в области противодействия техническим разведкам и технической защиты информации, применительно к сфере их деятельности, сведения, указанные в пункте 7 части 3 статьи 22 настоящего Федерального закона;

6) направлять заявление в орган, осуществляющий лицензирование деятельности оператора, для рассмотрения вопроса о принятии мер по приостановлению действия или аннулированию соответствующей лицензии в установленном законодательством Российской Федерации порядке, если условием лицензии на осуществление такой деятельности является запрет на передачу персональных данных третьим лицам без согласия в письменной форме субъекта персональных данных;

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

8) вносить в Правительство Российской Федерации предложения о совершенствовании нормативного правового регулирования защиты прав субъектов персональных данных;

9) привлекать к административной ответственности лиц, виновных в нарушении настоящего Федерального закона.

4. В отношении персональных данных, ставших известными уполномоченному органу по защите прав субъектов персональных данных в ходе осуществления им своей деятельности, должна обеспечиваться конфиденциальность персональных данных.

5. Уполномоченный орган по защите прав субъектов персональных данных обязан:

1) организовывать в соответствии с требованиями настоящего Федерального закона и других федеральных законов защиту прав субъектов персональных данных;

2) рассматривать жалобы и обращения граждан или юридических лиц по вопросам, связанным с обработкой персональных данных, а также принимать в пределах своих полномочий решения по результатам рассмотрения указанных жалоб и обращений;

3) вести реестр операторов;

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

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

6) информировать государственные органы, а также субъектов персональных данных по их обращениям или запросам о положении дел в области защиты прав субъектов персональных данных;

7) выполнять иные предусмотренные законодательством Российской Федерации обязанности.

5.1. Уполномоченный орган по защите прав субъектов персональных данных осуществляет сотрудничество с органами, уполномоченными по защите прав субъектов персональных данных в иностранных государствах, в частности международный обмен информацией о защите прав субъектов персональных данных, утверждает перечень иностранных государств, обеспечивающих адекватную защиту прав субъектов персональных данных.

6. Решения уполномоченного органа по защите прав субъектов персональных данных могут быть обжалованы в судебном порядке.

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

8. Финансирование уполномоченного органа по защите прав субъектов персональных данных осуществляется за счет средств федерального бюджета.

9. При уполномоченном органе по защите прав субъектов персональных данных создается на общественных началах консультативный совет, порядок формирования и порядок деятельности которого определяются уполномоченным органом по защите прав субъектов персональных данных.

Статья 24. Ответственность за нарушение требований настоящего Федерального закона

1. Лица, виновные в нарушении требований настоящего Федерального закона, несут предусмотренную законодательством Российской Федерации ответственность.

2. Моральный вред, причиненный субъекту персональных данных вследствие нарушения его прав, нарушения правил обработки персональных данных, установленных настоящим Федеральным законом, а также требований к защите персональных данных, установленных в соответствии с настоящим Федеральным законом, подлежит возмещению в соответствии с законодательством Российской Федерации. Возмещение морального вреда осуществляется независимо от возмещения имущественного вреда и понесенных субъектом персональных данных убытков.

Глава 6. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

Статья 25. Заключительные положения

1. Настоящий Федеральный закон вступает в силу по истечении ста восьмидесяти дней после дня его официального опубликования.

2. После дня вступления в силу настоящего Федерального закона обработка персональных данных, включенных в информационные системы персональных данных до дня его вступления в силу, осуществляется в соответствии с настоящим Федеральным законом.

2.1. Операторы, которые осуществляли обработку персональных данных до 1 июля 2011 года, обязаны представить в уполномоченный орган по защите прав субъектов персональных данных сведения, указанные в пунктах 5, 7.1, 10 и 11 части 3 статьи 22 настоящего Федерального закона, не позднее 1 января 2013 года.

4. Операторы, которые осуществляют обработку персональных данных до дня вступления в силу настоящего Федерального закона и продолжают осуществлять такую обработку после дня его вступления в силу, обязаны направить в уполномоченный орган по защите прав субъектов персональных данных, за исключением случаев, предусмотренных частью 2 статьи 22 настоящего Федерального закона, уведомление, предусмотренное частью 3 статьи 22 настоящего Федерального закона, не позднее 1 января 2008 года.

5. Отношения, связанные с обработкой персональных данных, осуществляемой государственными органами, юридическими лицами, физическими лицами при предоставлении государственных и муниципальных услуг, исполнении государственных и муниципальных функций в субъекте Российской Федерации - городе федерального значения Москве, регулируются настоящим Федеральным законом, если иное не предусмотрено Федеральным законом "Об особенностях регулирования отдельных правоотношений в связи с присоединением к субъекту Российской Федерации - городу федерального значения Москве территорий и о внесении изменений в отдельные законодательные акты Российской Федерации".

Президент
Российской Федерации
В.ПУТИН

Москва, Кремль
27 июля 2006 года

Федеральный закон РФ № 2487-1 от 11 марта 1992 года
«О частной детективной и охранной деятельности
в Российской Федерации»
(с изменениями и дополнениями)

Закон РФ от 11 марта 1992 г. N 2487-I «О частной детективной и охранной деятельности в Российской Федерации» (с изменениями от 21 марта 2002 г., 10 января 2003 г., 6 июня 2005 г., 18 июля 2006 г., 24 июля 2007 г., 22 декабря 2008 г., 25 ноября, 27 декабря 2009 г., 15 ноября 2010 г., 7 февраля, 1 июля, 3 декабря 2011 г.)

Раздел I Общие положения

Статья 1. Частная детективная и охранная деятельность

Настоящим Законом частная детективная и охранная деятельность определяются как оказание на возмездной договорной основе услуг физическим и юридическим лицам, имеющими специальное разрешение (лицензию) органов внутренних дел организациями и индивидуальными предпринимателями в целях защиты законных прав и интересов своих клиентов.

На граждан, осуществляющих частную детективную и охранную деятельность, действие законов, закрепляющих правовой статус работников правоохранительных органов, не распространяется.

Граждане, занимающиеся частной детективной деятельностью, не вправе осуществлять какие-либо оперативно-розыскные действия, отнесенные законом к исключительной компетенции органов, которым такое право предоставлено.

Иностранные граждане, граждане Российской Федерации, имеющие гражданство иностранного государства, иностранные юридические лица, а также организации, в составе учредителей (участников) которых имеются указанные граждане и лица, могут осуществлять частную детективную и охранную деятельность и (или) принимать участие в ее осуществлении в любой форме, в том числе в управлении частной охранной организацией, только на основаниях и в рамках, предусмотренных международными договорами Российской Федерации.

Статья 1.1. Основные понятия

В целях настоящего Закона используются следующие основные понятия:

1) частная охранная организация (далее также – охранная организация) – организация, специально учрежденная для оказания охранных услуг, зарегистрированная в установленном законом порядке и имеющая лицензию на осуществление частной охранной деятельности;

2) частный охранник – гражданин Российской Федерации, достигший восемнадцати лет, прошедший профессиональную подготовку для работы в качестве частного охранника, сдавший квалификационный экзамен, получивший в установленном настоящим Законом порядке удостоверение частного охранника и работающий по трудовому договору с охранной организацией;

3) удостоверение частного охранника – документ, дающий право частному охраннику работать по трудовому договору с охранной организацией на должности, связанной непосредственно с оказанием охранных услуг;

4) частный детектив – гражданин Российской Федерации, зарегистрированный в качестве индивидуального предпринимателя, получивший в установленном настоящим Законом порядке лицензию на осуществление частной детективной (сыскной) деятельности и оказывающий услуги, предусмотренные Частью 2 Статьи 3 настоящего Закона;

5) объекты охраны – недвижимые вещи (включая здания, строения, сооружения), движимые вещи (включая транспортные средства, грузы, денежные средства, ценные бумаги), в том числе при их транспортировке;

6) внутриобъектовый режим – порядок, устанавливаемый клиентом или заказчиком, не противоречащий законодательству Российской Федерации, доведенный до сведения персонала и посетителей объектов охраны и обеспечиваемый совокупностью мероприятий и правил, выполняемых лицами, находящимися на объектах охраны, в соответствии с правилами внутреннего трудового распорядка и требованиями пожарной безопасности;

7) пропускной режим – порядок, устанавливаемый клиентом или заказчиком, не противоречащий законодательству Российской Федерации, доведенный до сведения персонала и посетителей объектов охраны и обеспечиваемый совокупностью мероприятий и правил, исключающих возможность бесконтрольного входа (выхода) лиц, въезда (выезда) транспортных средств, вноса (выноса), ввоза (вывоза) имущества на объекты охраны (с объектов охраны).

Статья 2. Правовая основа частной детективной и охранной деятельности

Правовую основу частной детективной и охранной деятельности составляют Конституция Российской Федерации, настоящий Закон, другие законы и иные правовые акты Российской Федерации.

Статья 3. Виды охранных и сыскных услуг

Частная детективная и охранная деятельность осуществляется для сыска и охраны.

В целях сыска разрешается предоставление следующих видов услуг:

1) сбор сведений по гражданским делам на договорной основе с участниками процесса;

2) изучение рынка, сбор информации для деловых переговоров, выявление некредитоспособных или ненадежных деловых партнеров;

3) установление обстоятельств неправомерного использования в предпринимательской деятельности фирменных знаков и наименований, недобросовестной конкуренции, а также разглашения сведений, составляющих коммерческую тайну;

4) выяснение биографических и других характеризующих личность данных об отдельных гражданах (с их письменного согласия) при заключении ими трудовых и иных контрактов;

5) поиск без вести пропавших граждан;

6) поиск утраченного гражданами или предприятиями, учреждениями, организациями имущества;

7) сбор сведений по уголовным делам на договорной основе с участниками процесса. В течение суток с момента заключения контракта с клиентом на сбор таких сведений частный детектив обязан письменно уведомить об этом лицо, производящее дознание, следователя или суд, в чьем производстве находится уголовное дело;

8) поиск лица, являющегося должником в соответствии с исполнительным документом, его имущества, а также поиск ребенка по исполнительному документу, содержащему требование об отобрании ребенка, на договорной основе с взыскателем.

В целях охраны разрешается предоставление следующих видов услуг:

1) защита жизни и здоровья граждан;

2) охрана объектов и (или) имущества (в том числе при его транспортировке), находящихся в собственности, во владении, в пользовании, хозяйственном ведении, опе-

ративном управлении или доверительном управлении, за исключением объектов и (или) имущества, предусмотренных Пунктом 7 настоящей части;

3) охрана объектов и (или) имущества на объектах с осуществлением работ по проектированию, монтажу и эксплуатационному обслуживанию технических средств охраны, перечень видов которых устанавливается Правительством Российской Федерации, и (или) с принятием соответствующих мер реагирования на их сигнальную информацию;

4) консультирование и подготовка рекомендаций клиентам по вопросам правомерной защиты от противоправных посягательств;

5) обеспечение порядка в местах проведения массовых мероприятий.

6) обеспечение внутриобъектового и пропускного режимов на объектах, за исключением объектов, предусмотренных пунктом 7 настоящей части;

7) охрана объектов и (или) имущества, а также обеспечение внутриобъектового и пропускного режимов на объектах, которые имеют особо важное значение для обеспечения жизнедеятельности и безопасности государства и населения и перечень которых утверждается в порядке, установленном Правительством Российской Федерации.

В порядке, установленном Правительством Российской Федерации, организациям, осуществляющим частную охранную деятельность, предоставляется право содействовать правоохранительным органам в обеспечении правопорядка, а частным детективам предоставляется право содействовать правоохранительным органам в предупреждении и раскрытии преступлений, предупреждении и пресечении административных правонарушений.

Физическим и юридическим лицам, не имеющим правового статуса частного детектива, частного охранника или частной охранной организации, запрещается оказывать услуги, предусмотренные настоящей статьей.

Раздел II Частная детективная (сыскная) деятельность

Статья 4. Смешанные формы детективной и охранной деятельности – утратила силу

Статья 5. Действия частных детективов

В ходе частной сыскной деятельности допускаются устный опрос граждан и должностных лиц (с их согласия), наведение справок, изучение предметов и документов (с письменного согласия их владельцев), внешний осмотр строений, помещений и других объектов, наблюдение для получения необходимой информации в целях оказания услуг, перечисленных в части первой статьи 3 настоящего Закона.

При осуществлении частной сыскной деятельности допускается использование видео- и аудиозаписи, кино- и фотосъемки, технических и иных средств, не причиняющих вреда жизни и здоровью граждан и окружающей среде, в соответствии с законодательством Российской Федерации.

В ходе осуществления своей деятельности частный детектив обязан соблюдать законодательство Российской Федерации в части защиты информации, затрагивающей личную жизнь и имущество граждан.

Статья 6. Предоставление лицензий частным детективам

Предоставление лицензий на осуществление частной детективной деятельности производится органами внутренних дел. Лицензия предоставляется сроком на пять лет и действительна на всей территории Российской Федерации. Решение о предоставлении либо об отказе в предоставлении лицензии принимается в срок не более сорока пяти дней. Правительством Российской Федерации утверждается положение о лицензировании частной детективной деятельности, в котором устанавливаются порядок лицензирования данного вида деятельности и перечень лицензионных требований и условий.

Гражданин, претендующий на получение лицензии на осуществление частной детективной деятельности, обязан лично представить в соответствующий орган внутренних дел заявление, в котором указываются его фамилия, имя и (в случае, если имеется) отчество, государственный регистрационный номер записи о государственной регистрации индивидуального предпринимателя и данные документа, подтверждающего факт внесения записи об индивидуальном предпринимателе в единый государственный реестр индивидуальных предпринимателей, предполагаемая территория осуществления частной детективной деятельности, и следующие документы:

– анкету;

– фотографии;

– медицинскую справку о состоянии здоровья;

– документы, подтверждающие его гражданство, наличие юридического образования или прохождение профессиональной подготовки для работы в качестве частного сыщика, либо стаж работы в оперативных или следственных подразделениях не менее трех лет;

– сведения о потребности в технических средствах и намерении их использовать.

Органы внутренних дел вправе устанавливать достоверность сведений, изложенных в представленных документах, необходимых для принятия решения о выдаче лицензии, в том числе путем собеседования с гражданином, претендующим на ее получение, а также запрашивать соответствующие правоохранительные, лицензирующие, контролирующие и надзорные органы.

Лицензия не предоставляется:

1) гражданам, не достигшим двадцати одного года;

2) гражданам, состоящим на учете в органах здравоохранения по поводу психического заболевания, алкоголизма или наркомании;

3) гражданам, имеющим судимость за совершение умышленного преступления;

4) гражданам, которым предъявлено обвинение в совершении преступления (до разрешения вопроса об их виновности в установленном законом порядке);

5) гражданам, уволенным с государственной службы, из судебных, прокурорских и иных правоохранительных органов по компрометирующим их основаниям;

6) бывшим работникам правоохранительных органов, осуществлявшим контроль за частной детективной и охранной деятельностью, если со дня их увольнения не прошел год;

7) гражданам, не представившим документы, перечисленные в Части 2 настоящей статьи.

8) гражданам, в отношении которых по результатам проверки, проведенной в соответствии с законодательством Российской Федерации, имеется заключение о невозможности допуска к осуществлению частной детективной деятельности в связи с повышенной опасностью нарушения прав и свобод граждан, возникновением угрозы общественной безопасности, подготовленное в порядке, установленном Правительством Российской Федерации, и утвержденное руководителем уполномоченного на осуществление действий по лицензированию частной детективной деятельности подразделения федерального органа исполнительной власти, в ведении которого находятся вопросы внутренних дел, его заместителями либо министром внутренних дел, начальником управления (главного управления) внутренних дел по субъекту Российской Федерации или лицами, исполняющими обязанности указанных должностных лиц;

9) гражданам, не прошедшим обязательной государственной дактилоскопической регистрации.

В случае отказа в выдаче лицензии орган внутренних дел обязан письменно информировать об этом гражданина, направившего заявление, с указанием мотивов отка-

за. Это решение или нарушение срока рассмотрения заявления может быть обжаловано в вышестоящий орган внутренних дел или суд.

Гражданину, получившему лицензию на осуществление частной детективной деятельности, одновременно выдается удостоверение частного детектива.

Органы внутренних дел осуществляют следующие полномочия в области лицензирования частной детективной деятельности:

1) предоставление лицензии и выдача удостоверения частного детектива;

2) переоформление документов, подтверждающих наличие лицензии;

3) приостановление и возобновление действия лицензии в случаях, установленных настоящим Законом;

4) ведение реестров лицензий и предоставление сведений из них;

5) осуществление государственного контроля за соблюдением лицензиатами лицензионных требований и условий;

6) обращение в суд с заявлением о приостановлении действия лицензии либо об аннулировании лицензии;

7) прекращение действия лицензии в случае получения письменного заявления лицензиата о прекращении им осуществления данного вида деятельности.

На частных детективов распространяется установленный настоящим Законом для лицензирования частной охранной деятельности порядок приостановления действия лицензий и аннулирования лицензий, оформления и переоформления документов, подтверждающих наличие лицензии.

К отношениям, связанным с лицензированием и не урегулированным настоящим Законом, применяются положения законодательства Российской Федерации.

Грубыми нарушениями осуществления частной детективной деятельности считаются:

1) совершение лицензиатом в ходе оказания сыскных услуг действий, которые повлекли за собой нарушение прав граждан на неприкосновенность жилища, тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений;

2) оказание лицензиатом сыскных услуг с использованием запрещенных к применению технических средств;

3) оказание лицензиатом в целях сыска услуг, не предусмотренных Частью 2 Статьи 3 настоящего Закона либо оказываемых без заключения договора, предусмотренного Статьей 9 настоящего Закона;

4) необеспечение доступа должностных лиц лицензирующего органа при проведении ими проверочных мероприятий, предусмотренных Статьей 20 настоящего Закона, в места хранения технических средств и (или) служебной документации.

Статья 7. Ограничения в сфере деятельности частного детектива

Частным детективам запрещается:

1) скрывать от правоохранительных органов ставшие им известными факты готовящихся, совершаемых или совершенных преступлений;

2) выдавать себя за сотрудников правоохранительных органов;

3) собирать сведения, связанные с личной жизнью, с политическими и религиозными убеждениями отдельных лиц;

4) осуществлять видео- и аудиозапись, фото- и киносъемку в служебных или иных помещениях без письменного согласия на то соответствующих должностных или частных лиц;

5) прибегать к действиям, посягающим на права и свободы граждан;

6) совершать действия, ставящие под угрозу жизнь, здоровье, честь, достоинство и имущество граждан;

7) фальсифицировать материалы или вводить в заблуждение клиента;

8) разглашать собранные в ходе выполнения договорных обязательств сведения о заказчике, в том числе сведения, касающиеся вопросов обеспечения защиты жизни и здоровья граждан и (или) охраны имущества заказчика, использовать их в каких-либо целях вопреки интересам заказчика или в интересах третьих лиц, кроме как на основаниях, предусмотренных законодательством Российской Федерации;

9) передавать свою лицензию для использования ее другими лицами;

10) использовать документы и иные сведения, полученные в результате осуществления оперативно-розыскной деятельности органами, уполномоченными в данной сфере деятельности;

11) получать и использовать информацию, содержащуюся в специальных и информационно-аналитических базах данных органов, осуществляющих оперативно-розыскную деятельность, в нарушение порядка, установленного законодательством Российской Федерации.

Проведение сыскных действий, нарушающих тайну переписки, телефонных переговоров и телеграфных сообщений либо связанных с нарушением гарантий неприкосновенности личности или жилища, влечет за собой установленную законом ответственность.

Сыскная деятельность должна быть основным видом деятельности частного детектива, совмещение ее с государственной службой либо муниципальной службой или с замещением выборной оплачиваемой должности в общественном объединении не разрешается.

Статья 8. Утратила силу с 1 января 2010 г.

Статья 9. Особенности требований к договору на оказание сыскных услуг

1) Частный детектив обязан заключить с каждым из своих заказчиков договор на оказание сыскных услуг в письменной форме, в котором должны быть отражены сведения о договаривающихся сторонах, в том числе номер и дата выдачи лицензии, вид и содержание оказываемых услуг, срок их оказания, стоимость услуг или порядок ее определения.

2) Договор на оказание сыскных услуг и акт о выполнении работ подлежат хранению в течение пяти лет.

Статья 10. Статья полностью исключена

Раздел III Частная охранная деятельность

Статья 11. Оказание услуг в сфере охраны

1) Оказание услуг, перечисленных в Части 3 Статьи 3 настоящего Закона, разрешается только организациям, специально учреждаемым для их выполнения и имеющим лицензию, выданную органами внутренних дел.

2) О начале и об окончании оказания охранных услуг, изменении состава учредителей (участников) частная охранная организация обязана уведомить органы внутренних дел в порядке, установленном Правительством Российской Федерации.

3) Охранная деятельность организаций не распространяется на объекты, подлежащие государственной охране, перечень которых утверждается Правительством Российской Федерации. Охранным организациям разрешается оказывать услуги в виде вооруженной охраны имущества в порядке, установленном Правительством Российской Федерации, а также использовать технические и иные средства, не причиняющие вреда жизни и здоровью граждан и окружающей среде, средства оперативной радио- и телефонной связи.

4) Запрещается вооруженная охрана имущества на территориях закрытых административно-территориальных образований, а также приобретение и использование ору-

жия частными охранными организациями, зарегистрированными и (или) расположенными на их территориях.

Пункт 5 утратил силу с 1 января 2010 г.

Статья 11.1. Правовой статус частного охранника

Право на приобретение правового статуса частного охранника предоставляется гражданам, прошедшим профессиональную подготовку и сдавшим квалификационный экзамен, и подтверждается удостоверением частного охранника. Порядок сдачи квалификационного экзамена и выдачи удостоверения частного охранника устанавливается Правительством Российской Федерации. Частный охранник работает по трудовому договору с частной охранной организацией, и его трудовая деятельность регулируется трудовым законодательством и настоящим Законом. Частный охранник в соответствии с полученной квалификацией пользуется предусмотренными настоящим Законом правами только в период выполнения трудовой функции в качестве работника частной охранной организации.

Не вправе претендовать на приобретение правового статуса частного охранника лица:

1) не являющиеся гражданами Российской Федерации;

2) не достигшие восемнадцати лет;

3) признанные решением суда недееспособными или ограниченно дееспособными;

4) имеющие заболевания, которые препятствуют исполнению ими обязанностей частного охранника. Перечень таких заболеваний устанавливается Правительством Российской Федерации;

5) имеющие судимость за совершение умышленного преступления;

6) которым предъявлено обвинение в совершении преступления (до разрешения вопроса об их виновности в установленном законом порядке);

7) не прошедшие профессиональной подготовки для работы в качестве охранника;

8) в отношении которых по результатам проверки, проведенной в соответствии с законодательством Российской Федерации, имеется заключение о невозможности допуска к осуществлению частной охранной деятельности в связи с повышенной опасностью нарушения прав и свобод граждан, возникновением угрозы общественной безопасности, подготовленное в порядке, установленном Правительством Российской Федерации, и утвержденное руководителем уполномоченного на осуществление действий по лицензированию частной охранной деятельности подразделения федерального органа исполнительной власти, в ведении которого находятся вопросы внутренних дел, его заместителями либо министром внутренних дел, начальником управления (главного управления) внутренних дел по субъекту Российской Федерации или лицами, исполняющими обязанности указанных должностных лиц;

9) досрочно прекратившие полномочия по государственной должности или уволенные с государственной службы, в том числе из правоохранительных органов, из органов прокуратуры, судебных органов, по основаниям, которые в соответствии с законодательством Российской Федерации связаны с совершением дисциплинарного проступка, грубым или систематическим нарушением дисциплины, совершением проступка, порочащего честь государственного служащего, утратой доверия к нему, если после такого досрочного прекращения полномочий или такого увольнения прошло менее трех лет;

10) у которых удостоверение частного охранника было аннулировано по основаниям, указанным в Пункте 1 Части 4 настоящей статьи, если после принятия решения об аннулировании прошло менее года;

11) не прошедшие обязательной государственной дактилоскопической регистрации в порядке, установленном законодательством Российской Федерации.

Удостоверение частного охранника выдается сроком на пять лет. Срок действия удостоверения частного охранника может продлеваться в порядке, установленном Правительством Российской Федерации. Продление срока действия удостоверения частного охранника осуществляется только после повышения квалификации в образовательных учреждениях, указанных в Статье 15.2 настоящего Закона.

Удостоверение частного охранника аннулируется в случае:

1) неоднократного привлечения в течение года частного охранника к административной ответственности за совершение административных правонарушений, посягающих на институты государственной власти, административных правонарушений против порядка управления и административных правонарушений, посягающих на общественный порядок и общественную безопасность;

2) возникновения обстоятельств, при которых гражданин не может претендовать на приобретение правового статуса частного охранника;

3) окончания срока действия удостоверения частного охранника, добровольного отказа от такого удостоверения либо смерти гражданина, которому было выдано такое удостоверение.

Удостоверение частного охранника аннулируется по решению органа внутренних дел. Порядок его изъятия устанавливается федеральным органом исполнительной власти, в ведении которого находятся вопросы внутренних дел.

За выдачу удостоверения (дубликата удостоверения) частного охранника, а также за переоформление и внесение изменений в удостоверение частного охранника уплачивается государственная пошлина в размерах и порядке, которые установлены законодательством Российской Федерации о налогах и сборах.

Статья 11.2. Лицензирование частной охранной деятельности

Предоставление лицензий на осуществление частной охранной деятельности производится органами внутренних дел. Лицензия предоставляется сроком на пять лет и действует на всей территории Российской Федерации. В лицензии указывается (указываются) вид (виды) охранных услуг, которые может оказывать лицензиат. Решение о предоставлении либо об отказе в предоставлении лицензии принимается в срок не более сорока пяти дней.

Правительством Российской Федерации утверждается положение о лицензировании частной охранной деятельности, в котором устанавливаются порядок лицензирования данного вида деятельности и перечень лицензионных требований и условий по каждому виду охранных услуг, предусмотренных Частью 3 Статьи 3 настоящего Закона.

Органы внутренних дел осуществляют следующие полномочия в области лицензирования частной охранной деятельности:

1) предоставление лицензии;

2) переоформление документов, подтверждающих наличие лицензии;

3) приостановление и возобновление действия лицензии в случаях, установленных настоящим Законом;

4) ведение реестров лицензий и предоставление сведений из них;

5) осуществление государственного контроля за соблюдением лицензиатами лицензионных требований и условий, а также требований законодательства Российской Федерации, регламентирующего оборот оружия и специальных средств;

6) обращение в суд с заявлением о приостановлении действия лицензии либо об аннулировании лицензии;

7) прекращение действия лицензии в случае получения письменного заявления лицензиата о прекращении им осуществления данного вида деятельности.

Статья 11.3. Предоставление юридическим лицам лицензий на осуществление частной охранной деятельности

Для получения лицензии на осуществление частной охранной деятельности руководитель организации обязан представить в соответствующий орган внутренних дел:

1) заявление о предоставлении лицензии на осуществление частной охранной деятельности, в котором указываются полное наименование юридического лица, его организационно-правовая форма, место его нахождения, предполагаемый (предполагаемые) вид (виды) охранных услуг, намерение использовать технические и иные средства, оружие, специальные средства и потребность в них;

2) документы по каждому виду охранных услуг, предусмотренные положением о лицензировании частной охранной деятельности;

3) документ, подтверждающий уплату государственной пошлины за предоставление лицензии.

К заявлению могут быть приложены:

1) копии учредительных документов;

2) копия свидетельства о государственной регистрации юридического лица;

3) копия свидетельства о постановке на учет в налоговом органе.

В случае, если документы, указанные в Пунктах 2 и 3 Части 2 настоящей статьи, не представлены руководителем организации, по межведомственному запросу органа внутренних дел федеральный орган исполнительной власти, осуществляющий государственную регистрацию юридических лиц, физических лиц в качестве индивидуальных предпринимателей и крестьянских (фермерских) хозяйств, предоставляет сведения, подтверждающие факт внесения сведений о юридическом лице в единый государственный реестр юридических лиц, а федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору за соблюдением законодательства о налогах и сборах, предоставляет сведения, подтверждающие факт постановки юридического лица на учет в налоговом органе.

Порядок и условия представления документов в органы внутренних дел устанавливаются Правительством Российской Федерации в положении о лицензировании частной охранной деятельности.

Копии документов, не заверенные в установленном порядке, представляются вместе с оригиналами.

Органы внутренних дел обязаны устанавливать достоверность сведений, изложенных в представленных документах и приложениях к ним.

Основанием для отказа в предоставлении лицензии является несоответствие соискателя лицензии лицензионным требованиям и условиям.

Статья 11.4. Переоформление документа, подтверждающего наличие лицензии на осуществление частной охранной деятельности

Документ, подтверждающий наличие лицензии на осуществление частной охранной деятельности, подлежит переоформлению в случае:

1) продления срока действия лицензии;

2) намерения лицензиата осуществлять новый (новые) вид (виды) охранных услуг, не указанный (не указанные) в предоставленной лицензии;

3) реорганизации охранной организации;

4) изменения наименования охранной организации или места ее нахождения.

В случае продления срока действия лицензии или намерения лицензиата осуществлять новый (новые) вид (виды) охранных услуг представляются соответствующее заявление и документы по данному виду услуг, предусмотренные положением о лицензировании частной охранной деятельности.

В случае реорганизации охранной организации либо изменения ее наименования или места нахождения данная охранная организация в течение пятнадцати суток с даты внесения соответствующих изменений в единый государственный реестр юридических лиц либо с даты изменения своего места нахождения обязана подать в орган внутренних дел, выдавший лицензию, соответствующее заявление. Для рассмотрения заявления необходимы документы, подтверждающие указанные обстоятельства. В случае, если документы, подтверждающие реорганизацию охранной организации либо изменение ее наименования или места нахождения, не представлены заявителем самостоятельно, по межведомственному запросу органа внутренних дел федеральный орган исполнительной власти, осуществляющий государственную регистрацию юридических лиц, физических лиц в качестве индивидуальных предпринимателей и крестьянских (фермерских) хозяйств, предоставляет сведения, подтверждающие факт внесения соответствующих сведений о юридическом лице в единый государственный реестр юридических лиц. При этом в течение трех суток с даты подачи в регистрирующий орган заявления о государственной регистрации, связанной с реорганизацией охранной организации либо с изменением ее наименования или места нахождения, данная охранная организация в порядке, установленном положением о лицензировании частной охранной деятельности, обязана уведомить об указанных обстоятельствах орган внутренних дел, выдавший лицензию.

Переоформление документа, подтверждающего наличие лицензии на осуществление частной охранной деятельности, производится в порядке, предусмотренном для предоставления лицензии, в срок не более тридцати дней.

На период переоформления действие лицензии не приостанавливается.

Статья 11.5. Приостановление действия лицензии и аннулирование лицензии

Органы внутренних дел вправе приостанавливать действие лицензии в случае выявления неоднократных нарушений или грубого нарушения лицензиатом лицензионных требований и условий, указанных в Части 9 настоящей статьи. При этом устанавливается срок устранения выявленных нарушений, повлекших за собой приостановление действия лицензии, который не может быть более месяца. Приостановление действия лицензии за не являющиеся грубыми неоднократные нарушения лицензионных требований и условий не допускается без предварительных письменных предупреждений лицензиата и без предоставления ему времени для устранения указанных нарушений.

В случае, если в установленный срок лицензиат не устранил нарушение лицензионных требований и условий, орган внутренних дел обязан обратиться в суд с заявлением о приостановлении действия лицензии на срок до шести месяцев либо об аннулировании лицензии.

Срок действия лицензии на время приостановления ее действия не продлевается.

Лицензия может быть аннулирована решением суда на основании заявления органа внутренних дел в случае, если нарушение лицензиатом лицензионных требований и условий повлекло за собой нарушение прав, законных интересов, нанесение ущерба здоровью граждан, обороне и безопасности государства, культурному наследию народов Российской Федерации, а также в случае неустранения лицензиатом в установленный срок выявленных нарушений.

Одновременно с подачей заявления в суд орган внутренних дел вправе приостановить действие лицензии на период до вступления в силу решения суда.

Право принятия решения о приостановлении действия лицензии предоставляется в порядке, установленном Правительством Российской Федерации, руководителю федерального органа исполнительной власти, в ведении которого находятся вопросы внутренних дел, его заместителям, руководителю уполномоченного на осуществление дей-

ствий по лицензированию частной охранной деятельности подразделения данного федерального органа исполнительной власти, его заместителям либо министру внутренних дел, начальнику управления (главного управления) внутренних дел по субъекту Российской Федерации или лицам, исполняющим обязанности указанных должностных лиц.

Решение о приостановлении действия лицензии либо об аннулировании лицензии может быть обжаловано в порядке, установленном законодательством Российской Федерации.

Грубыми нарушениями осуществления частной охранной деятельности считаются:

1) нарушение в охранной организации правил оборота оружия, установленных законодательством Российской Федерации, если такое нарушение:

- повлекло за собой утрату, хищение оружия либо его использование в преступных целях;
- выразилось в выдаче оружия работнику охранной организации, не имеющему разрешения на хранение и ношение служебного оружия, либо лицу, не являющемуся работником данной охранной организации;

2) нарушение в охранной организации правил оборота оружия и (или) специальных средств, установленных законодательством Российской Федерации, если такое нарушение повлекло за собой нарушение прав, законных интересов, нанесение ущерба здоровью граждан либо иные тяжкие последствия;

3) оказание лицензиатом охранных услуг в виде вооруженной охраны имущества без заключения соответствующего договора либо без уведомления органов внутренних дел о начале оказания охранных услуг, а также оказание лицензиатом охранных услуг с использованием специальных средств без заключения соответствующего договора и без уведомления органов внутренних дел о начале оказания охранных услуг;

4) оказание лицензиатом услуг, не предусмотренных имеющейся у него лицензией, либо услуг, не предусмотренных частью 3 статьи 3 настоящего Закона;

5) необеспечение доступа должностных лиц органа внутренних дел в ходе проведения ими проверочных мероприятий, предусмотренных Статьей 20 настоящего Закона, в места хранения оружия, специальных средств и (или) служебной документации, отражающей учет и использование оружия и (или) специальных средств, либо воспрепятствование такому доступу.

Статья 11.6. Ведение реестров лицензий

Ведение реестров лицензий на осуществление частной охранной деятельности и предоставление сведений из них осуществляются в порядке, установленном Правительством Российской Федерации.

Статья 12. Дополнительные условия осуществления частной охранной деятельности

Работникам частной охранной организации не разрешается совмещать охранную деятельность с государственной службой либо с выборной оплачиваемой должностью в общественных объединениях.

Работником частной охранной организации не может быть учредитель (участник), руководитель либо иное должностное лицо организации, с которой данной частной охранной организацией заключен договор на оказание охранных услуг.

В случае оказания охранных услуг с использованием видеонаблюдения, а также оказания охранных услуг в виде обеспечения внутриобъектового и (или) пропускного режимов персонал и посетители объекта охраны должны быть проинформированы об этом посредством размещения соответствующей информации в местах, обеспечивающих гарантированную видимость в дневное и ночное время, до входа на охраняемую территорию. Такая информация должна содержать сведения об условиях внутриобъектового и пропускного режимов.

Заключение охранными организациями договоров с клиентами на оказание охранных услуг осуществляется в соответствии с положениями Статьи 9 настоящего Закона, при этом к договору прилагаются копии заверенных заказчиком документов, подтверждающих его право владения или пользования имуществом, подлежащим охране, в соответствии с законодательством Российской Федерации.

На охранную деятельность распространяются ограничения, установленные Статьей 7 настоящего Закона. Охранникам запрещается использовать методы сыска.

Лицо, совершившее противоправное посягательство на охраняемое имущество, может быть задержано охранником на месте правонарушения и должно быть незамедлительно передано в орган внутренних дел (полицию).

Обязательным требованием является наличие у работников частной охранной организации, осуществляющих охранные услуги, личной карточки охранника, выданной органами внутренних дел в порядке, установленном федеральным органом исполнительной власти, в ведении которого находятся вопросы внутренних дел. Работники частной охранной организации имеют право оказывать охранные услуги в специальной форменной одежде, если иное не оговорено в договоре с заказчиком. Оказание работниками частной охранной организации услуг в специальной форменной одежде должно позволять определять их принадлежность к конкретной частной охранной организации.

Специальная форменная одежда и знаки различия работников частных охранных организаций не могут быть аналогичными форме одежды и знакам различия сотрудников правоохранительных органов и военнослужащих, а также сходными с ними до степени смешения. Порядок ношения специальной форменной одежды при оказании различных видов охранных услуг устанавливается Правительством Российской Федерации.

Специальная раскраска, информационные надписи и знаки на транспортных средствах частных охранных организаций подлежат согласованию с органами внутренних дел в порядке, установленном Правительством Российской Федерации.

Статья 12.1. Обеспечение внутриобъектового и пропускного режимов на объектах охраны

В соответствии с договором на оказание охранных услуг, заключенным охранной организацией с клиентом или заказчиком, частные охранники при обеспечении внутриобъектового и пропускного режимов в пределах объекта охраны, а также при транспортировке охраняемых грузов, денежных средств и иного имущества имеют право:

1) требовать от персонала и посетителей объектов охраны соблюдения внутриобъектового и пропускного режимов. Правила соблюдения внутриобъектового и пропускного режимов, устанавливаемые клиентом или заказчиком, не должны противоречить законодательству Российской Федерации;

2) осуществлять допуск лиц на объекты охраны, на которых установлен пропускной режим, при предъявлении ими документов, дающих право на вход (выход) лиц, въезд (выезд) транспортных средств, внос (вынос), ввоз (вывоз) имущества на объекты охраны (с объектов охраны);

3) производить в пределах, установленных законодательством Российской Федерации, на объектах охраны, на которых установлен пропускной режим, осмотр въезжающих на объекты охраны (выезжающих с объектов охраны) транспортных средств, за исключением транспортных средств оперативных служб государственных военизированных организаций, в случае возникновения подозрения, что указанные транспортные средства используются в противоправных целях, а также осмотр вносимого на объекты охраны (выносимого с объектов охраны) имущества. Осмотр указанных транспортных средств и имущества должен производиться в присутствии водителей указанных транспортных средств и лиц, сопровождающих указанные транспортные средства и имущество;

4) применять физическую силу, специальные средства и огнестрельное оружие в случаях и порядке, которые установлены законодательством Российской Федерации;

5) оказывать содействие правоохранительным органам в решении возложенных на них задач.

Действия частных охранников на объектах охраны регламентируются должностной инструкцией частного охранника. Типовые требования к должностной инструкции частного охранника утверждаются федеральным органом исполнительной власти, в ведении которого находятся вопросы внутренних дел. Экземпляр должностной инструкции частного охранника в обязательном порядке направляется в орган внутренних дел по месту нахождения соответствующего объекта охраны.

Частные охранники при обеспечении внутриобъектового и пропускного режимов обязаны:

1) руководствоваться должностной инструкцией частного охранника;

2) соблюдать конституционные права и свободы человека и гражданина, права и законные интересы физических и юридических лиц;

3) обеспечивать защиту объектов охраны от противоправных посягательств;

4) незамедлительно сообщать руководителю частной охранной организации и в соответствующие правоохранительные органы ставшую им известной информацию о готовящихся либо совершенных преступлениях, а также о действиях, об обстоятельствах, создающих на объектах охраны угрозу безопасности людей;

5) предъявлять по требованию сотрудников правоохранительных органов, других граждан удостоверение частного охранника.

Частным охранникам запрещается препятствовать законным действиям должностных лиц правоохранительных и контролирующих органов при осуществлении указанными должностными лицами своей деятельности.

Раздел IV Смешанные формы детективной и охранной деятельности

Утратил силу с 1 января 2010 г.

Раздел IV.1 Требования к частным охранным организациям и учреждениям по подготовке частных детективов и работников частных охранных организаций

Статья 15.1. Требования к частным охранным организациям

Частная охранная организация может быть создана только в форме общества с ограниченной ответственностью и не может осуществлять иную деятельность, кроме охранной. Уставный капитал частной охранной организации не может быть менее ста тысяч рублей. Для частной охранной организации, оказывающей (намеренной оказывать) услуги по вооруженной охране имущества и (или) услуги, предусмотренные Пунктом 3 Части 3 Статьи 3 настоящего Закона, уставный капитал не может быть менее двухсот пятидесяти тысяч рублей. Предельный размер имущественных (неденежных) вкладов в уставный капитал частной охранной организации не может быть более 50 процентов от размера уставного капитала. Не могут быть использованы для формирования уставного капитала частной охранной организации привлеченные денежные средства.

Внесение в уставный капитал частной охранной организации средств иностранными гражданами, гражданами Российской Федерации, имеющими гражданство иностранного государства, лицами без гражданства, иностранными юридическими лицами, а также организациями, в составе учредителей (участников) которых имеются указанные граждане и лица, запрещается, если иное не предусмотрено международными договорами Российской Федерации.

Отчуждение долей (вкладов) учредителем (участником) частной охранной организации, повлекшее за собой появление в уставном капитале доли (вклада) с иностранным участием, не допускается, если иное не предусмотрено международными договорами Российской Федерации.

Частная охранная организация не может являться дочерним обществом организации, осуществляющей иную деятельность, кроме охранной. Для учредителя (участника) частной охранной организации данный вид деятельности должен быть основным. Право учреждения частной охранной организации юридическим лицом, осуществляющим иную деятельность, кроме охранной, может быть предоставлено при наличии достаточных оснований в порядке, установленном Правительством Российской Федерации. Филиалы частной охранной организации могут создаваться только в том субъекте Российской Федерации, на территории которого частная охранная организация зарегистрирована.

Учредителями (участниками) частной охранной организации не могут являться:

1) общественные объединения;

2) физические и (или) юридические лица, не соответствующие требованиям, указанным в части четвертой настоящей статьи;

3) граждане, состоящие на государственной службе либо замещающие выборные оплачиваемые должности в общественных объединениях;

4) граждане, имеющие судимость за совершение умышленного преступления, а также юридические лица, в составе учредителей (участников) которых имеются указанные лица;

5) иностранные граждане, граждане Российской Федерации, имеющие гражданство иностранного государства, лица без гражданства, иностранные юридические лица, а также организации, в составе учредителей (участников) которых имеются указанные граждане и лица, при отсутствии соответствующего международного договора Российской Федерации.

Участниками частной охранной организации могут оставаться учредившие ее лица, которые получили право на пенсию по старости в соответствии с законодательством Российской Федерации, перешли на работу в общественные организации, работающие в сфере частной охранной либо частной детективной деятельности, либо назначены (избраны) на государственные должности Российской Федерации. Лицам, назначенным (избранным) на указанные государственные должности, запрещается принимать участие в управлении охранной организацией.

Руководитель частной охранной организации должен иметь высшее профессиональное образование и пройти повышение квалификации для руководителей частных охранных организаций. Обязательным требованием является наличие у руководителя частной охранной организации удостоверения частного охранника.

Руководитель частной охранной организации не вправе замещать государственные должности Российской Федерации, государственные должности субъектов Российской Федерации, должности государственной службы, выборные оплачиваемые должности в общественных объединениях, а также вступать в трудовые отношения в качестве работника, за исключением осуществления им научной, преподавательской и иной творческой деятельности.

Статья 15.2. Требования к образовательным учреждениям, осуществляющим профессиональную подготовку частных детективов, частных охранников и руководителей частных охранных организаций

Профессиональная подготовка и повышение квалификации частных детективов осуществляются в образовательных учреждениях среднего профессионального и высшего профессионального образования.

Профессиональная подготовка и повышение квалификации частных охранников осуществляются в образовательных учреждениях дополнительного профессионального, начального профессионального, среднего профессионального и высшего профессионального образования.

Повышение квалификации руководителей частных охранных организаций осуществляется на базе образовательных учреждений дополнительного профессионального, среднего профессионального и высшего профессионального образования.

Учредителями (участниками) негосударственных образовательных учреждений, осуществляющих подготовку частных детективов и работников частных охранных организаций, не могут являться:

1) граждане, имеющие судимость за совершение умышленного преступления, а также юридические лица, в составе учредителей (участников) которых имеются указанные лица;

2) иностранные граждане, граждане Российской Федерации, имеющие гражданство иностранного государства, лица без гражданства, иностранные юридические лица, а также организации, в составе учредителей (участников) которых имеются указанные граждане и лица, при отсутствии соответствующего международного договора Российской Федерации.

Указанные в настоящей статье образовательные учреждения должны иметь на основаниях, предусмотренных законодательством Российской Федерации, стрелковые объекты для проведения занятий по огневой подготовке. Порядок проведения соответствующих стрельб определяется федеральным органом исполнительной власти, в ведении которого находятся вопросы внутренних дел.

Статья 15.3. Профессиональная подготовка частных детективов, частных охранников и руководителей частных охранных организаций

Требования к минимуму содержания профессиональных образовательных программ подготовки и повышения квалификации частных детективов, частных охранников и руководителей частных охранных организаций устанавливаются федеральным органом исполнительной власти, осуществляющим функции по выработке и реализации государственной политики и нормативно-правовому регулированию в сфере образования, по согласованию с федеральным органом исполнительной власти, в ведении которого находятся вопросы внутренних дел.

Обучение частных детективов и работников частных охранных организаций в заочной форме и в форме экстерната не допускается.

Раздел V Применение специальных средств и огнестрельного оружия при осуществлении частной детективной и охранной деятельности

Статья 16. Условия применения специальных средств и огнестрельного оружия

В ходе осуществления частной охранной деятельности разрешается применять огнестрельное оружие и специальные средства только в случаях и порядке, предусмотренных настоящим Законом. Виды, типы, модели, количество огнестрельного оружия и патронов к нему, порядок их приобретения и обращения, а также виды и модели специальных средств, порядок их приобретения, учета, хранения и ношения регламентируются Правительством Российской Федерации. Норма обеспечения служебным огнестрельным оружием определяется с учетом потребности в нем, связанной с оказанием охранных услуг, и не может быть более одной единицы на двух частных охранников.

Охранник при применении специальных средств или огнестрельного оружия обязан:

- предупредить о намерении их использовать, предоставив при этом достаточно времени для выполнения своих требований, за исключением тех случаев, когда про-

медление в применении специальных средств или огнестрельного оружия создает непосредственную опасность его жизни и здоровью или может повлечь за собой иные тяжкие последствия;

- стремиться в зависимости от характера и степени опасности правонарушения и лиц, его совершивших, а также силы оказываемого противодействия к тому, чтобы любой ущерб, причиненный при устранении опасности, был минимальным;
- обеспечить лицам, получившим телесные повреждения, первую помощь и уведомить о происшедшем в возможно короткий срок органы здравоохранения и внутренних дел;
- немедленно уведомить прокурора о всех случаях смерти или причинения телесных повреждений.

Частные охранники обязаны проходить периодические проверки на пригодность к действиям в условиях, связанных с применением огнестрельного оружия и (или) специальных средств. Содержание периодических проверок, порядок и сроки их проведения определяются федеральным органом исполнительной власти, в ведении которого находятся вопросы внутренних дел.

Применение охранником специальных средств или огнестрельного оружия с превышением своих полномочий, крайней необходимости или необходимой обороны влечет за собой ответственность, установленную законом.

Статья 17. Применение специальных средств

На частную охранную деятельность распространяются правила применения специальных средств, установленные Правительством Российской Федерации для органов внутренних дел Российской Федерации.

Частные охранники имеют право применять специальные средства в следующих случаях:

1) для отражения нападения, непосредственно угрожающего их жизни и здоровью;

2) для пресечения преступления против охраняемого ими имущества, когда правонарушитель оказывает физическое сопротивление.

Запрещается применять специальные средства в отношении женщин с видимыми признаками беременности, лиц с явными признаками инвалидности и несовершеннолетних, когда их возраст очевиден или известен частному охраннику, кроме случаев оказания ими вооруженного сопротивления, совершения группового либо иного нападения, угрожающего жизни и здоровью частного охранника или охраняемому имуществу.

Статья 18. Применение огнестрельного оружия

Охранники имеют право применять огнестрельное оружие в следующих случаях:

1) для отражения нападения, когда его собственная жизнь подвергается непосредственной опасности;

2) для отражения группового или вооруженного нападения на охраняемое имущество;

3) для предупреждения (выстрелом в воздух) о намерении применить оружие, а также для подачи сигнала тревоги или вызова помощи.

Запрещается применять огнестрельное оружие в отношении женщин, лиц с явными признаками инвалидности и несовершеннолетних, когда их возраст очевиден или известен охраннику, кроме случаев оказания ими вооруженного сопротивления, совершения вооруженного либо группового нападения, угрожающего жизни охранника или охраняемому имуществу, а также при значительном скоплении людей, когда от применения оружия могут пострадать посторонние лица.

О каждом случае применения огнестрельного оружия охранник обязан незамедлительно информировать орган внутренних дел по месту применения оружия.

Раздел VI Гарантии социальной и правовой защиты лиц, занимающихся частной детективной и охранной деятельностью

Статья 19. Социальная и правовая защита частных детективов и охранников

Частная детективная и охранная деятельность засчитывается в общий трудовой стаж и стаж для назначения пособий по государственному социальному страхованию при условии уплаты взносов в Пенсионный фонд Российской Федерации и в Фонд государственного социального страхования Российской Федерации.

Граждане, занимающиеся частной охранной деятельностью, подлежат страхованию на случай гибели, получения увечья или иного повреждения здоровья в связи с оказанием ими охранных услуг в порядке, установленном законодательством Российской Федерации. Указанное страхование граждан, занимающихся частной охранной деятельностью, осуществляется за счет средств соответствующей охранной организации и включается в состав ее затрат.

Оказание сопротивления, угроза или насилие в отношении лиц, занимающихся оказанием охранных услуг в связи с исполнением ими своих обязанностей, влечет ответственность в соответствии с законом.

Раздел VII Контроль и надзор за частной детективной и охранной деятельностью

Статья 20. Контроль и надзор за частной детективной и охранной деятельностью

Контроль за частной детективной и охранной деятельностью на территории Российской Федерации осуществляют федеральный орган исполнительной власти, в ведении которого находятся вопросы внутренних дел, иные федеральные органы исполнительной власти и подчиненные им органы и подразделения в пределах, установленных настоящим Законом, другими законами и иными правовыми актами Российской Федерации.

Должностные лица, уполномоченные осуществлять контроль за деятельностью частных детективов, охранных организаций, образовательных учреждений, осуществляющих профессиональную подготовку частных детективов и работников частных охранных организаций, по вопросам, отнесенным к компетенции органов внутренних дел, в порядке, установленном законодательством Российской Федерации, вправе требовать от них в рамках своей компетенции представления соответствующих документов и получать письменную или устную информацию, необходимую для выполнения контрольных функций.

Надзор за исполнением настоящего Закона осуществляют Генеральный прокурор Российской Федерации и подчиненные ему прокуроры.

Должностные лица органов внутренних дел имеют право проводить проверку прохождения подготовки частных охранников и руководителей охранных организаций, предусмотренной Частью 6 Статьи 12 Федерального закона от 13 декабря 1996 года N 150-ФЗ «Об оружии».

В целях осуществления государственного контроля за соблюдением лицензиатом лицензионных требований и условий орган внутренних дел в пределах своей компетенции проводит плановую и внеплановую проверки. Указанные проверки проводятся на основании распоряжений (приказов) органа внутренних дел.

Проверка наличия, организации хранения и учета огнестрельного оружия, патронов и специальных средств проводится в соответствии с законодательством Российской Федерации, регламентирующим оборот оружия и специальных средств.

Плановая проверка может проводиться не чаще одного раза в 3 года. Продолжительность ее проведения не должна превышать месяц. О проведении внеплановой проверки в обязательном порядке уведомляется прокурор субъекта Российской Федерации.

Внеплановая проверка проводится в следующих случаях:

1) если в результате проведения плановой проверки выявлены нарушения лицензионных требований и условий;

2) если от органов государственной власти и органов контроля (надзора) получена информация о создающем угрозу здоровью и жизни граждан нарушении лицензиатом законодательства Российской Федерации, регламентирующего деятельность частных детективов и частных охранных организаций;

3) если имеются обращения граждан и (или) юридических лиц с жалобами на нарушение их прав и законных интересов действиями (бездействием) лицензиата либо его работников, а также если получена иная информация, подтверждаемая документами и другими доказательствами, свидетельствующими о наличии такого нарушения.

По результатам проверки осуществляющее ее должностное лицо составляет акт установленной формы, копия которого вручается руководителю охранной организации, частному детективу или его представителю под расписку либо направляется посредством почтовой связи с уведомлением о вручении.

К отношениям, связанным с проведением органами внутренних дел проверок лицензиатов и не урегулированным настоящим Законом, применяются положения законодательства Российской Федерации.

Раздел VIII Ответственность за осуществление незаконной частной детективной и охранной деятельности

Статья 21. Ответственность за осуществление незаконной частной детективной и охранной деятельности

Нарушение установленных настоящим Законом требований к осуществлению частной детективной и охранной деятельности, а также условий ее осуществления влечет за собой ответственность в соответствии с законодательством Российской Федерации.

Раздел IX Осуществление частной охранной деятельности в связи с организацией и проведением XXII Олимпийских зимних игр и XI Паралимпийских зимних игр 2014 года в городе Сочи

Статья 22. Осуществление частной охранной деятельности в связи с организацией и проведением XXII Олимпийских зимних игр и XI Паралимпийских зимних игр 2014 года в городе Сочи

Осуществление частной охранной деятельности в связи с организацией и проведением XXII Олимпийских зимних игр и XI Паралимпийских зимних игр 2014 года в городе Сочи регулируется настоящим Законом, если иное не определено Федеральным законом от 30 октября 2007 года N 238-ФЗ «О Государственной корпорации по строительству олимпийских объектов и развитию города Сочи как горноклиматического курорта».

Президент Российской Федерации Б.Ельцин

Москва, Дом Советов России
11 марта 1992 года
N 2487-I