

**Типовые требования
к содержанию и порядку разработки Руководства
по защите информации от технических разведок
и от ее утечки по техническим каналам на объекте
(одобreno решением от 03.10.95 г. № 42 Гостехкомиссии России)**

1. ОБЩИЕ ПОЛОЖЕНИЯ.

1.1. Настоящий документ устанавливает единые типовые требования к содержанию и порядку разработки Руководства по защите информации от технических разведок и от ее утечки по техническим каналам (далее - Руководство) на строящемся (реконструируемом), действующем (находящемся в эксплуатации) объекте. Под объектом защиты (далее - объект) понимается имущественный комплекс: здания, сооружения, помещения и территория, на которой они размещены, а также расположенные в них технические средства и иное имущество, требующее защиты и принадлежащее государственным органам, государственным и коммерческим организациям (в том числе НИИ, КБ, опытный или серийный завод, испытательный центр, полигон, воинская часть и т.п.) на праве собственности, оперативного управления или хозяйственного ведения.

1.2. В соответствии с требованиями Положения о государственной системе защиты информации в Российской Федерации от иностранных технических разведок и от ее утечки по техническим каналам, утвержденного постановлением Совета Министров - Правительства Российской Федерации от 15 сентября 1993 года №912-51, Руководство разрабатывается на каждом объекте, на котором предусматривается защита информации от технических разведок и от ее утечки по техническим каналам (далее - защита информации) в ходе его строительства (реконструкции) и эксплуатации.

1.3. Руководство определяет содержание и порядок осуществления мероприятий по защите информации, содержащей сведения, отнесенные в установленном порядке к государственной или служебной тайне. Мероприятия по защите информации должны быть увязаны с мероприятиями по легендированию объектов и режиму секретности.

1.4. При разработке Руководства используются:

- концепция защиты информации от иностранной технической разведки (ИТР);
 - модель иностранной технической разведки применительно к объекту защиты;
 - нормы противодействия средствам иностранной технической разведки;
 - нормы эффективности защиты информации, обрабатываемой техническими средствами;
 - инструкция по защите информации об образцах вооружения и военной техники, создаваемых или используемых на объекте;
 - требования по защите информации о создаваемых образцах вооружения и военной техники и выполняемых работах, подлежащих защите от ИТР;
 - инструкция по проектированию технических мероприятий защиты промышленных объектов от ИТР;
 - проектная документация на строительство (реконструкцию) объекта в части мер защиты информации в ходе его эксплуатации, общий маскировочный замысел защиты информации для объектов первой категории;
 - результаты анализа разведдоступности и аттестования объекта (первая, вторая, третья категории) или его составных частей на соответствие требованиям по защите информации;
 - методические и другие руководящие документы в области защиты информации.
- При разработке Руководства данные об осведомленности разведок в отношении

конкретного объекта получают в соответствующем министерстве (ведомстве).

• •2. ОСНОВНОЕ СОДЕРЖАНИЕ РУКОВОДСТВА ПО ЗАЩИТЕ ИНФОРМАЦИИ •

•2.1. Руководство должно состоять из следующих разделов:

- общие положения;
- охраняемые сведения об объекте;
- демаскирующие признаки объекта и технические каналы утечки информации;
- оценка возможностей технических разведок и других источников угроз безопасности информации (возможно спецтехника, используемая преступными группировками);
- организационные и технические мероприятия по защите информации;
- оповещение о ведении разведки (раздел включается в состав Руководства при необходимости);
- обязанности и права должностных лиц;
- планирование работ по защите информации и контролю;
- контроль состояния защиты информации;
- аттестование рабочих мест;
- взаимодействие с другими предприятиями (учреждениями, организациями).

•В зависимости от особенностей объекта допускается вводить и другие разделы.

•2.2. В разделе "Общие положения" указывается назначение Руководства, приводятся общие требования по защите информации на объекте, указывается категория объекта по требованиям обеспечения защиты информации, указываются должностные лица, ответственные за выполнение требований Руководства, определяется порядок финансирования работ по защите информации на объекте, приводятся сведения о полученной лицензии на допуск к работе со сведениями, составляющими государственную тайну и об имеющихся сертифицированных средствах защиты информации.

•2.3. В разделе "Охраняемые сведения об объекте" указывается конкретная цель, которая должна быть достигнута в результате проведения мероприятий по защите информации (охраняемых сведений) об объекте, замысел достижения этой цели и приводится перечень охраняемых сведений об объекте и его деятельности (без указания конкретных числовых параметров).

•2.4. В разделе "Демаскирующие признаки объекта" и технические каналы утечки информации" указываются демаскирующие признаки, которые раскрывают охраняемые сведения об объекте, в том числе демаскирующие признаки, возникающие в связи с использованием средств обеспечения его деятельности. Приводятся возможные технические каналы утечки охраняемых сведений об объекте, включая каналы утечки информации в технических средствах ее обработки.

•2.5. В разделе "Оценка возможностей иностранных технических разведок и других источников угроз безопасности информации" приводится перечень видов и средств технической разведки, источников угроз несанкционированного доступа к информации, которые опасны для данного объекта, в том числе со стороны преступных группировок и результаты оценки их возможностей:

- по обнаружению (определению) демаскирующих признаков объекта, раскрывающих охраняемые сведения;
- по перехвату информации, циркулирующей в технических средствах ее обработки;
- по перехвату речевой информации из помещений;
- по получению, разрушению (уничтожению), искажению или блокированию информации в

результате несанкционированного доступа к ней.

- При оценке используется Модель иностранной технической разведки, Методики оценки возможностей иностранной технической разведки и другие документы по этому вопросу.

- 2.6. В разделе "Организационные и технические мероприятия по защите информации" приводятся организационные и технические мероприятия, обеспечивающие устранение или ослабление (искажение) демаскирующих признаков и закрытие возможных технических каналов утечки охраняемых сведений об объекте, мероприятия по защите информации о создаваемых (применяемых) образцах вооружения и военной техники в соответствии с Инструкциями по защите информации на эти образцы, мероприятия по защите информации об иной создаваемой (применяемой) продукции и технологиях, мероприятия по защите информации при постоянном контролируемом и неконтролируемом нахождении иностранных граждан, как на территории объекта, так и в непосредственной близости от него, а также мероприятия по защите информации в системах и средствах информатизации и связи. При нахождении на территории объекта организации, арендующей территорию данного объекта, требования по защите информации на данный объект должны быть включены в договор аренды.

- 2.7. В разделе "Оповещение о ведении разведки" указывается порядок получения, регистрации и передачи данных о пролетах разведывательных ИСЗ, самолетов иностранных авиакомпаний, на хождении иностранных судов в открытых портах, местах, маршрутах и времени проведения иностранных инспекций в соответствии с международными договорами, посещении объекта иностранными представителями, появлении в районе дислокации объекта иностранных граждан, подозреваемых в ведении разведки. А также приводятся внутри объектовая схема оповещения и действия должностных лиц при оповещении.

- 2.8. В разделе "Обязанности и права должностных лиц" определяются должностные лица подразделений объекта, ответственные за разработку, обеспечение и выполнение мероприятий по защите информации, их функциональные обязанности и права, приводится структурная схема взаимодействия подразделений по защите информации на объекте с соответствующими подразделениями данного объекта.

- 2.9. В разделе "Планирование работ по защите информации и контролю" указываются основные руководящие документы для планирования работ по защите информации, требования к содержанию планов, приводится порядок разработки, согласования, утверждения и оформления планов, устанавливается порядок отчетности и контроля за выполнением планов.

- 2.10. В разделе "Контроль состояния защиты информации" указываются задачи контроля, перечень органов и подразделений, имеющих право проверки состояния защиты информации на объекте, привлекаемые силы и средства контроля, порядок привлечения (при необходимости) к этой работе специалистов основных подразделений объекта, устанавливаются периодичность и виды контроля, порядок оформления результатов контроля, определяются действия должностных лиц по устранению нарушений норм и требований по защите информации и порядок разработки мероприятий по устранению указанных нарушений.

- 2.11. В разделе "Аттестование рабочих мест" указываются подразделения или должностные лица, ответственные за аттестование рабочих мест, стендов, вычислительных комплексов, выделенных помещений и т.д., приводится форма документирования результатов аттестования и порядок выдачи разрешения на проведение работ с секретной информацией, а также порядок и периодичность их переаттестования.

•2.12. В разделе "Взаимодействие с другими предприятиями (учреждениями, организациями)" указываются порядок взаимодействия в области защиты информации с предприятиями (учреждениями, организациями) при выполнении совместных работ, применяемые совместные организационные и технические мероприятия по защите информации, ответственность, права и обязанности взаимодействующих сторон, а также приводится структурная схема взаимодействия.

•2.13. В приложения к Руководству могут включаться:

- таблицы, схемы, графики, расчеты, исходные данные и другие справочные материалы для оценки обстановки, определения мероприятий по защите информации;
- перечень создаваемых (применяемых) образцов вооружения и военной техники, выполняемых НИОКР и другой продукции, подлежащих защите;
- перечень сведений, подлежащих защите;
- план объекта с указанием схем размещения рабочих мест,
- стендов и т.д., и схем организации связи и сигнализации объекта;
- структура системы защиты информации на объекте;
- перечень руководящих, нормативных и методических документов по защите информации и др.

Корректировка приложений должна проводиться в случаях изменения характера и направленности работ, разведобстановки, влияющих на состояние защиты охраняемых сведений, введения в действие новых нормативных документов по защите информации или уточнений к ним, а также при уточнении (изменении) легенд прикрытия.

3. ПОРЯДОК РАЗРАБОТКИ, СОГЛАСОВАНИЯ И УТВЕРЖДЕНИЯ РУКОВОДСТВА ПО ЗАЩИТЕ ИНФОРМАЦИИ

3.1. Руководство по защите информации разрабатывается подразделением по защите информации от иностранных технических разведок и от ее утечки по техническим каналам совместно с основными подразделениями объекта. При отсутствии подразделения или отдельных специалистов по защите информации разработку Руководства организует руководитель объекта по договору с предприятиями, организациями, имеющими лицензию на данный вид деятельности. Руководство подписывается должностным лицом, ответственным за защиту информации на объекте и утверждается руководителем объекта по согласованию с представителем заказчика, головным подразделением отрасли по защите информации (для предприятий, входящих в состав ведомств) и соответствующим территориальным органом государственной безопасности. Согласованное Руководство утверждается руководителем органа государственной власти или предприятия (учреждения, организации).

3.2. Изменения в Руководство вносятся, согласовываются и утверждаются в том же порядке и на том же уровне, что и основной документ.

3.3. К ознакомлению с Руководством в полном объеме допускается строго ограниченный круг лиц по решению руководителя объекта. Исполнители мероприятий по защите информации на объекте должны быть ознакомлены с Руководством в части, их касающейся.