Постановление Совета Министров — Правительства РФ от 15.09.1993 № 912-51 «Об утверждении Положения о государственной системе защиты информации в Российской Федерации от иностранных технических разведок и от ее утечки по техническим каналам»

1. Настоящее Положение является документом, обязательным для выполнения при проведении работ по защите информации, содержащей сведения, составляющие государственную или служебную тайну, в органах (аппаратах, администрациях) представительной, исполнительной и судебной властей Российской Федерации, республик в составе Российской Федерации, автономной области, автономных округов, краев, областей, городов Москвы и Санкт-Петербурга и в органах местного самоуправления (далее именуются органы государственной власти), на предприятиях и в их объединениях, учреждениях и организациях независимо от их организационно-правовой формы и формы собственности (далее именуются — предприятия).

2. Положение определяет структуру государственной системы защиты информации в Российской Федерации, ее задачи и функции, основы организации защиты сведений, отнесенных в установленном порядке к государственной или служебной тайне, от иностранных технических разведок и от ее утечки по техническим каналам (далее именуется защита информации).

3. Работы по защите информации в органах государственной власти и на предприятиях проводятся на основе актов законодательства Российской Федерации.

4. Защита информации осуществляется путем выполнения комплекса мероприятий по предотвращению утечки информации по техническим каналам, несанкционированного доступа к ней, предупреждению преднамеренных программнотехнических воздействий с целью разрушения (уничтожения) или искажения информации в процессе обработки, передачи и хранения по противодействию иностранным техническим разведкам, а также путем проведения специальных работ, порядок организации и выполнения которых определяется Советом министров Правительством Российской Федерации.

5. Мероприятия по защите информации являются составной частью управленческой, научной и производственной

деятельности и осуществляются во взаимосвязи с другими мерами по обеспечению установленного режима секретности проводимых работ.

6. Главными направлениями работ по защите информации являются:

обеспечение эффективного управления системой защиты информации;

определение сведений, охраняемых от технических средств разведки, и демаскирующих признаков, раскрывающих эти сведения;

анализ и оценка реальной опасности перехвата информации техническими средствами разведки, несанкционированного доступа, разрушения (уничтожения) или искажения информации путем преднамеренных программно-технических воздействий в процессе ее обработки, передачи и хранения в технических средствах, выявление возможных технических каналов утечки сведений, подлежащих защите;

разработка организационно-технических мероприятий по защите информации и их реализация;

организация и проведение контроля состояния защиты информации.

7. Основными организационно-техническими мероприятиями по защите информации являются:

лицензирование деятельности предприятий в области защиты информации;

аттестование объектов по выполнению требований обеспечения защиты информации при проведении работ со сведениями соответствующей степени секретности;

сертификация средств защиты информации и контроля за ее эффективностью, систем и средств информатизации и связи в части защищенности информации от утечки по техническим каналам;

категорирование вооружения и военной техники, предприятий (объектов) по степени важности защиты информации в оборонной, экономической, политической, научно-технической и других сферах деятельности государства;

обеспечение условий защиты информации при подготовке и реализации международных договоров и соглашений;

оповещение о пролетах космических и воздушных летательных аппаратов, кораблях и судах, ведущих разведку

объектов (перехват информации, подлежащей защите), расположенных на территории Российской Федерации;

введение территориальных, частотных, энергетических, пространственных и временных ограничений в режимах использования технических средств, подлежащих защите;

создание и применение информационных и автоматизированных систем управления в защищенном исполнении;

разработка и внедрение технических решений и элементов защиты информации при создании и эксплуатации вооружения и военной техники, при проектировании, строительстве (реконструкции) и эксплуатации объектов, систем и средств информатизации и связи;

разработка средств защиты информации и контроля за ее эффективностью (специального и общего применения) и их использование;

применение специальных методов, технических мер и средств защиты, исключающих перехват информации передаваемой по каналам связи.

8. Конкретные методы, приемы и меры защиты информации разрабатываются в зависимости от степени возможного ущерба в случае ее утечки, разрушения (уничтожения).

9. Проведение любых мероприятий и работ с использованием сведений, отнесенных к государственной или служебной тайне, без принятия необходимых мер по защите информации не допускается.

II. Государственная система защиты информации

10. Основные задачи государственной системы защиты информации:

проведение единой технической политики, организация и координация работ по защите информации в оборонной, экономической, политической, научно-технической и других сферах деятельности;

исключение или существенное затруднение добывания информации техническими средствами разведки, а также предотвращение ее утечки по техническим каналам, несанкционированного доступа к ней, предупреждение преднамеренных программно-технических воздействий с целью разрушения (уничтожения) или искажения информации в

процессе ее обработки, передачи и хранения;

принятие в пределах компетенции правовых актов, регулирующих отношения в области защиты информации;

анализ состояния и прогнозирования возможностей технических средств разведки и способов их применения, формирование системы информационного обмена сведениями по осведомленности иностранных разведок;

организация сил, создание средств защиты информации и контроля за ее эффективностью;

контроль состояния защиты информации в органах государственной власти и на предприятиях.

…

18. Организация работ по защите информации на предприятиях осуществляется их руководителями.

В зависимости от объема работ по защите информации руководителем предприятия создается структурное подразделение по защите информации либо назначаются штатные специалисты по этим вопросам.

Подразделения по защите информации (штатные специалисты) на предприятиях осуществляют мероприятия по защите информации в ходе выполнения работ с использованием сведений, отнесенных к государственной или служебной тайне, определяют совместно с заказчиком работ основные направления комплексной защиты информации, участвуют в согласовании технических (тактико-технических) заданий на проведения работ с информацией, содержащей сведения, отнесенные к государственной и служебной тайне.

Указанные подразделения (штатные специалисты) подчиняются непосредственно руководителю предприятия или его заместителю. Работники этих подразделений (штатные специалисты) приравниваются по оплате труда к соответствующим категориям работников основных структурных подразделений.

Для проведения работ по защите информации могут привлекаться на договорной основе специализированные предприятия, имеющие лицензии на право проведения работ в области защиты информации.

19. Предприятия, имеющие намерения нормативно

заниматься деятельностью в области защиты информации, должны получить соответствующую лицензию на определенный вид этой деятельности. Лицензии выдаются Государственной технической комиссией при Президенте Российской Федерации и Федеральным агентством правительственной связи и информации при Президенте Российской Федерации в соответствии со своей компетенцией по представлению органа государственной власти.

20. Высшие учебные заведения и институты повышения квалификации по подготовке и переподготовке кадров в области защиты информации осуществляют:

первичную подготовку специалистов по комплексной защите информации;

переподготовку (повышение квалификации) специалистов по защите информации органов государственной власти и предприятий;

усовершенствование знаний руководителей органов государственной власти и предприятий в области защиты информации.

Подготовка кадров для государственной системы защиты информации осуществляется при методическом руководстве Государственной технической комиссии при Президенте Российской Федерации.

III. Организация защиты информации в системах и средствах информатизации и связи

21. Защита информации в системах и средствах информатизации и связи является составной частью работ по их созданию, эксплуатации и осуществляется во всех органах государственной власти и на предприятиях, располагающих информацией, содержащей сведения, отнесенные к государственной или служебной тайне.

22. Требования по защите информации в системах и средствах информатизации и связи определяются заказчиками совместно с разработчиками на стадии подготовки и согласования решений Совета Министров Правительства Российской Федерации, приказов и директив, планов и программ работ, технических и тактико-технических заданий на проведение исследований, разработку (модернизацию), испытания, производство и эксплуатацию (применение на

основе стандартов, нормативно-технических и методических документов, утверждаемых Комитетом Российской Федерации по стандартизации, метрологии и сертификации, Государственной технической комиссией при Президенте Российской Федерации и другими органами государственной власти в соответствии с их компетенцией. Указанные требования согласовываются с подразделениями по защите информации.

23. Организация защиты информации в системах и средствах информатизации и связи возлагается на руководителей органов государственной власти и предприятий, заказчиков и разработчиков систем и средств информатизации и связи, руководителей подразделений, эксплуатирующих эти системы и средства, ответственность за обеспечение защиты информации непосредственно на пользователя (потребителя) информации.

24. В интересах обеспечения защиты информации в системах и средствах информатизации и связи защите подлежат:

информационные ресурсы, содержащие сведения, отнесенные к государственной или служебной тайне, представленные в виде носителей на магнитной и оптической основе, информативных физических полей, информационных массивов и баз данных;

средства и системы информатизации (средства вычислительной техники, информационно-вычислительные комплексы, сети и системы), программные средства (операционные системы, системы управления базами данных, другое общесистемное и прикладное программное обеспечение) автоматизированные системы управления, системы связи и передачи данных, технические средства приема, передачи и обработки информации (звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки графической, смысловой и буквенно-цифровой информации), используемые для обработки информации, содержащей сведения, отнесенные к государственной или служебной тайне;

технические средства и системы, не обрабатывающие информацию, но размещенные в помещениях, где обрабатывается (циркулирует) информация, содержащая

сведения, отнесенные к государственной или служебной тайне, а также сами помещения, предназначенные для ведения секретных переговоров.

25. Целями защиты информации являются:

предотвращение утечки информации по техканалам;

предотвращение несанкционированного уничтожения, искажения, копирования, блокирования информации в системах информатизации;

соблюдение правового режима использования массивов, программ обработки информации, обеспечение полноты, целостности, достоверности информации в системах обработки;

сохранение возможности управления процессом обработки и пользования информацией.

26. Защита информации осуществляется путем:

предотвращения перехвата техническими средствами информации, передаваемой по каналам связи;

предотвращения утечки обрабатываемой информации за счет побочных электромагнитных излучений и наводок, создаваемых функционирующими техническими средствами, а также электроакустических преобразований;

исключения несанкционированного доступа к обрабатываемой или хранящейся в технических средствах информации;

предотвращения специальных программно-технических воздействий, вызывающих разрушение, уничтожение, искажение информации или сбои в работе средств информатизации;

выявления возможно внедренных на объекты и в технические средства электронных устройств перехвата информации (закладных устройств);

предотвращения перехвата техническими средствами речевой информации из помещений и объектов.

Предотвращение перехвата техническими средствами информации, передаваемой по каналам связи, достигается применением криптографических и иных методов и средств защиты, а также проведением организационно-технических и режимных мероприятий.

Предотвращение утечки обрабатываемой информации за счет побочных электромагнитных излучений и наводок, а также электроакустических преобразований достигается применением

защищенных технических средств, аппаратных средств защиты, средств активного противодействия, экранированием зданий или отдельных помещений, установлением контролируемой зоны вокруг средств информатизации и другими организационными и техническими мерами.

Исключение несанкционированного доступа к обрабатываемой или хранящейся в технических средствах информации достигается применением специальных программно-технических средств защиты, использованием криптографических способов защиты, а также организационными и режимными мероприятиями.

Предотвращение специальных программно-технических воздействий, вызывающих разрушение, уничтожение, искажение информации или сбои в работе средств информатизации, достигается применением специальных программных аппаратных средств защиты (антивирусные процессоры, антивирусные программы) организацией системы контроля безопасности программного обеспечения.

Выявление возможно внедренных на объекты и в технические средства электронных устройств перехвата информации (закладных устройств) достигается проведением специальных проверок по выявлению этих устройств.

Предотвращение перехвата техническими средствами речевой информации из помещений и объектов достигается применением специальных средств защиты, проектными решениями, обеспечивающими звукоизоляцию помещений, выявлением специальных устройств подслушивания и другими организационными и режимными мероприятиями.

27. Информация, содержащая сведения, отнесенные к государственной или служебной тайне, должна обрабатываться с использованием защищенных систем и средств информатизации и связи или с использованием технических и программных средств защиты, сертифицированных в установленном порядке.

Соответствие технического средства и его программного обеспечения требованиям защищенности подтверждается сертификатом, выдаваемым предприятием, имеющим лицензию на этот вид деятельности, по результатам сертификационных испытаний, или предписанием на эксплуатацию, оформляемым по результатам специальных исследований и специальных

проверок технических средств и программного обеспечения.

Для оценки готовности систем и средств информатизации и связи к обработке (передаче) информации, содержащей сведения, отнесенные к государственной или служебной тайне, проводится аттестование указанных систем и средств в реальных условиях эксплуатации на предмет соответствия принимаемых методов, мер и средств защиты требуемому уровню безопасности информации.

…

VI. Контроль состояния защиты информации

47. Контроль состояния защиты информации (далее именуется контроль) осуществляется с целью своевременного выявления и предотвращения утечки информации по техническим каналам, несанкционированного доступа к ней, преднамеренных программно-технических воздействий на информацию и оценки защиты ее от иностранных технических разведок.

Контроль заключается в проверке выполнения актов законодательства Российской Федерации по вопросам защиты информации, решений Государственной технической комиссии при Президенте Российской Федерации, а также в оценке обоснованности и эффективности принятых мер защиты для обеспечения выполнения утвержденных требований и норм по защите информации.

48. Контроль организуется Государственной технической комиссией при Президенте Российской Федерации, Министерством безопасности Российской Федерации, Министерством внутренних дел Российской Федерации, Министерством обороны Российской Федерации, Службой внешней разведки Российской Федерации и Федеральным агентством правительственной связи и информации при Президенте Российской Федерации, структурными и межотраслевыми подразделениями органов государственной власти, входящими в государственную систему защиты информации, и предприятиями в соответствии с их компетенцией.

Акты проверок предприятий рассылаются их руководителями в орган, проводивший проверку, и в орган государственной

власти по подчиненности предприятия.

49. Государственная техническая комиссия при Президенте Российской Федерации организует контроль силами центрального аппарата и подчиненных ей в специальном отношении специальных центров. Она может привлекать для этих целей подразделения по защите информации органов государственной власти.

Центральный аппарат Государственной технической комиссии при Президенте Российской Федерации осуществляет в органах государственной власти и на предприятиях, обеспечивает методическое руководство работами по контролю (за исключением объектов и технических средств, защита которых входит в компетенцию Министерства безопасности Российской Федерации, Министерства внутренних дел Российской Федерации, Министерства обороны Российской Федерации, Службы внешней разведки Российской Федерации, Федерального агентства правительственной связи и информации при Президенте Российской Федерации, Главного управления охраны Российской Федерации).

Специальные центры, подчиненные в специальном отношении Государственной технической комиссии при Президенте Российской Федерации, в пределах своей компетенции осуществляют контроль в органах государственной власти и на предприятиях, расположенных в зонах ответственности этих центров.

Контроль в органах государственной власти силами центрального аппарата Государственной технической комиссии при Президенте Российской Федерации и специальных центров, подаренных в специальном отношении Государственной технической комиссии при Президенте Российской Федерации, осуществляется по согласованию с соответствующими органами государственной власти.

50. Органы государственной власти организуют и осуществляют контроль на подчиненных им предприятиях через свои подразделения по защите информации. Повседневный контроль за состоянием защиты информации на предприятиях проводится силами их подразделений по защите информации.

51. Контроль на предприятиях негосударственного сектора при выполнении работ с использованием сведений, отнесенных к государственной или служебной тайне, осуществляется

органами государственной власти, Государственной технической комиссией при Президенте Российской Федерации, Министерством безопасности Российской Федерации, Федеральным агентством правительственной связи и информации при Президенте Российской Федерации и заказчиком работ в соответствии с их компетенцией.

52. Защита информации считается эффективной, если принимаемые меры соответствуют установленным требованиям или нормам.

Несоответствие мер установленным требованиям или нормам по защите информации является нарушением.

Нарушения по степени важности делятся на три категории:

первая невыполнение требований или норм по защите информации, в результате чего имелась или имеется реальная возможность ее утечки по техническим каналам;

вторая невыполнение требований по защите информации, в результате чего создаются предпосылки к ее утечке по техническим каналам;

третья невыполнение других требований по защите информации.

53. При обнаружении нарушений первой категории руководители органов государственной власти и предприятий обязаны:

немедленно прекратить работы на участке (рабочем месте), где обнаружены нарушения и принять меры по их устранению;

организовать в установленном порядке расследование причин и условий появления нарушений с целью недопущения их в дальнейшем и привлечения к ответственности виновных лиц;

сообщить в Государственную техническую комиссию при Президенте Российской Федерации, руководству органа государственной власти, федеральному органу государственной безопасности и заказчику о вскрытых нарушениях и принятых мерах.

Возобновление работ разрешается после устранения нарушений и проверки достаточности и эффективности принятых мер, проводимой Государственной технической комиссией при Президенте Российской Федерации или по ее поручению подразделениями по защите информации органов государственной власти.

При обнаружении нарушений второй и третьей категорий руководители проверяемых органов государственной власти и предприятий обязаны принять необходимые меры по их устранению в сроки, согласованные с органом, проводившим проверку, или заказчиком (представителем заказчика). Контроль за устранением этих нарушений осуществляется подразделениями по защите информации этих органов государственной власти и предприятий.

54. Допуск представителей центрального аппарата Государственной технической комиссии при Президенте Российской Федерации, специальных центров, подчиненных ей в специальном отношении, на объекты для проведения контроля состояния защиты информации, доступ их к работам и документам, необходимым для проведения контроля, осуществляется в установленном порядке по предъявлении специального удостоверения представителя Государственной технической комиссии при Президенте Российской Федерации и предписания на право проведения проверки данного объекта. Допуск на военные объекты осуществляется по разрешению начальника Генерального штаба Вооруженных Сил Российской Федерации.

Предписания на право проверки состояния защиты информации выдаются:

для объектов органов государственной власти председателем Государственной технической комиссии при Президенте Российской Федерации (заместителем председателя);

для предприятий на территории Российской Федерации начальником инспекции Государственной технической комиссией при Президенте Российской Федерации;

для предприятий в пределах установленных зон ответственности начальниками специальных центров, подчиненных в специальном отношении Государственной технической комиссии при Президенте Российской Федерации.

VII. Финансирование мероприятий по защите информации

55. Финансирование мероприятий по защите информации, содержащей сведения, отнесенные к государственной или служебной тайне, а также подразделений по защите

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

56. Создание технических средств защиты информации, не требующее капитальных вложений, осуществляется в пределах средств, выделяемых заказчиками на научно-исследовательские и опытно-конструкторские работы, связанные с разработкой продукции. Расходы по разработке технических средств защиты включаются в стоимость разработки образца продукции.

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