УТВЕРЖДЕНО
Указом Президента
Российской Федерации
от «___» _____ 20__ г. №___

ПОЛОЖЕНИЕ
о государственной системе защиты информации в Российской Федерации

I. Общие положения

1. Настоящее Положение определяет состав, направления деятельности государственной системы защиты информации в Российской Федерации (далее - государственная система защиты информации), а также требования к организации защиты информации ограниченного доступа и общедоступной информации, обладателями которой являются Российская Федерация, субъект Российской Федерации, муниципальное образование (далее — информация).

2. Требования настоящего Положения обязательны для исполнения федеральными органами исполнительной власти, органами исполнительной власти субъектов Российской Федерации, органами местного самоуправления, государственными фондами, государственными корпорациями (компаниями) при сборе, хранении, обработке, предоставлении, распространении ими информации (далее - обработка информации) с использованием объектов информационной инфраструктуры, а также организациями, осуществляющими на основании федеральных законов, иных нормативных правовых актов Российской Федерации, по договорам или на иных установленных законом основаниях обработку информации с использованием объектов информационной инфраструктуры (далее – органы, организации) на территории Российской Федерации.

3. В настоящем Положении используются следующие понятия:

безопасность информации — состояние информации и (или) объектов информационной инфраструктуры, обрабатывающих информацию, при котором обеспечиваются конфиденциальность, целостность, доступность информации;

защита информации — деятельность, направленная на предотвращение реализации (возникновения) угроз безопасности информации;

объекты информационной инфраструктуры — информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, иные объекты информатизации органа, организации;

средство защиты информации — программное (программно-аппаратное), техническое средство, предназначенное для защиты информации, средство, в котором оно реализовано, а также средство контроля эффективности защиты информации;

система организации и управления защитой информации — подразделения и работники, выполняющие функции по защите информации, и используемые ими средства защиты информации;

угроза безопасности информации — совокупность условий и факторов, создающих потенциально или реально существующую опасность нарушения безопасности информации.

4. Защита информации, содержащей сведения, составляющие государственную тайну, обеспечивается в соответствии с законодательством Российской Федерации о государственной тайне.

Организация защиты информации от иностранных технических разведок и от ее утечки по техническим каналам определяется Правительством Российской Федерации.

5. Защита информации в Министерстве обороны Российской Федерации, Федеральной службе безопасности Российской Федерации, Службе внешней разведки Российской Федерации и подведомственных им организациях осуществляется в порядке, установленном руководителями указанных федеральных органов исполнительной власти.

6. Защита информации, обрабатываемой объектами критической информационной инфраструктуры, обеспечивается в соответствии с настоящим Положением и законодательством Российской Федерации о безопасности критической информационной инфраструктуры.

II. Государственная система защиты информации

7. Государственная система защиты информации представляет собой функционирующий на федеральном, межрегиональном, региональном, ведомственном и объектовом уровнях организационный комплекс, включающий уполномоченные в области защиты информации федеральные органы исполнительной власти, подразделения и работников органов и организаций, выполняющих функции по защите информации, а также используемые ими средства защиты информации.

Организационную основу государственной системы защиты информации составляют:

Федеральная служба по техническому и экспортному контролю и ее территориальные органы, Федеральная служба безопасности Российской Федерации и территориальные органы безопасности - уполномоченные федеральные органы исполнительной власти;

органы, организации, организующие и (или) осуществляющие защиту информации в пределах полномочий, их подразделения, обеспечивающие защиту информации;

научные организации по проблемам защиты информации;

организации, осуществляющие создание средств защиты информации;

организации, выполняющие работы и (или) оказывающие услуги в области защиты информации;

органы по сертификации и испытательные центры (лаборатории), проводящие работы по сертификации (сертификационные испытания) средств защиты информации;

организации, осуществляющие подготовку кадров в области защиты информации.

8. Основными направлениями деятельности государственной системы защиты информации являются:

проведение единой государственной и научно-технической политики в области защиты информации, разработка нормативных правовых актов, методических документов и национальных стандартов в данной области;

координация деятельности органов, организаций по вопросам защиты информации на федеральном, межрегиональном, региональном, ведомственном и объектовом уровнях;

прогнозирование, выявление и оценка угроз безопасности информации, информирование органов, организаций об угрозах безопасности информации;

предотвращение несанкционированного доступа к информации и к объектам информационной инфраструктуры, обрабатывающим информацию, своевременное обнаружение фактов несанкционированного доступа;

недопущение воздействия на информацию и объекты информационной инфраструктуры, в результате которого нарушается безопасность обрабатываемой информации;

обеспечение возможности восстановления информации, модифицированной или уничтоженной вследствие несанкционированного доступа (воздействия) к ней и(или) к объектам информационной инфраструктуры, обрабатывающим информацию;

создание и внедрение способов, методов и средств защиты информации на основе применения передовых отечественных технологий, развитие отечественных конкурентоспособных средств защиты информации;

подготовка кадров в области защиты информации, повышение уровня знаний работников органов, организаций в данной области;

контроль обеспечения защиты информации и защищенности объектов информационной инфраструктуры (далее - контроль обеспечения защиты информации).

9. Уполномоченные федеральные органы исполнительной власти в пределах своих полномочий реализуют единую государственную и научно-техническую политику в области защиты информации, устанавливают требования о защите информации и осуществляют контроль обеспечения защиты информации, реализуют иные полномочия, установленные положениями об этих органах.

Федеральная служба по техническому и экспортному контролю во взаимодействии с Федеральной службой безопасности Российской Федерации организует деятельность государственной системы защиты информации.

10. Органы, организации организуют и обеспечивают защиту информации, обрабатываемой с использованием принадлежащих им объектов информационной инфраструктуры, в соответствии с требованиями о защите информации, установленными федеральными законами и принятыми в соответствии с ними иными нормативными правовыми актами Российской Федерации.

Органы организуют защиту информации в подведомственных им организациях.

11. Научные организации по проблемам защиты информации:

разрабатывают предложения по приоритетным направлениям исследований в области защиты информации, в том числе на основе анализа тенденций развития науки и техники;

разрабатывают прогнозы в области защиты информации исходя из текущего состояния и возможностей угроз безопасности информации;

проводят научно-исследовательские, опытно-конструкторские работы в области защиты информации;

выявляют, анализируют информацию об угрозах безопасности информации, разрабатывают предложения по методологии оценки угроз;

проводят исследования, направленные на создание и внедрение перспективных технологий, способов и методов защиты информации;

проводят работы по обоснованию требований к средствам защиты информации и направлениям их совершенствования;

разрабатывают предложения в проекты нормативных правовых актов, методических документов и национальных стандартов по защите информации;

осуществляют иные функции, установленные учредительными документами.

12. Организации, осуществляющие создание средств защиты информации, проводят работы по разработке, производству средств защиты информации в соответствии с требованиями по безопасности информации к средствам защиты информации и процессам их разработки, производства (далее — требования по безопасности информации), установленными уполномоченными федеральными органами исполнительной власти в пределах их полномочий, организуют их сертификацию на соответствие требованиям по безопасности информации в соответствии с законодательством Российской Федерации, а также обеспечивают техническую поддержку разработанных средств и обеспечивают устранение недостатков в разработанных ими средствах защиты информации.

13. Организации, выполняющие работы и (или) оказывающие услуги в области защиты информации, проводят работы в области защиты информации в соответствии с требованиями о защите информации, установленными уполномоченными федеральными органами исполнительной власти в пределах их полномочий, на основании лицензий, выданных уполномоченными федеральными органами исполнительной власти в соответствии с Федеральным законом «О лицензировании отдельных видов деятельности».

14. Органы по сертификации и испытательные центры (лаборатории) проводят сертификацию средств защиты информации на соответствие требованиям по безопасности информации, установленным уполномоченными федеральными органами исполнительной власти в пределах их полномочий. Организация и порядок проведения работ по сертификации средств защиты информации определяются в положениях о системах сертификации средств защиты информации, утвержденных уполномоченными федеральными органами исполнительной власти в пределах их полномочий.

15. Организации, осуществляющие подготовку кадров в области защиты информации, осуществляют подготовку, профессиональную переподготовку и (или) повышение квалификации специалистов в области защиты информации в соответствии с законодательством Российской Федерации об образовании.

Уполномоченные федеральные органы исполнительной власти в пределах полномочий осуществляют методическое руководство деятельностью по подготовке, профессиональной переподготовке, повышению квалификации специалистов в области защиты информации.

16. Деятельность государственной системы защиты информации осуществляется на федеральном, межрегиональном, региональном, ведомственном и объектовом уровнях.

На федеральном уровне межведомственную координацию деятельности в области защиты информации осуществляет Межведомственная комиссия Совета Безопасности Российской Федерации по информационной безопасности.

На межрегиональном уровне координацию деятельности в области защиты информации осуществляют комиссии по информационной безопасности, создаваемые при полномочных представителях Президента Российской Федерации в федеральных округах. Положение о комиссии утверждается полномочным представителем Президента Российской Федерации в федеральном округе на основе типового положения о комиссии по информационной безопасности, утвержденного Президентом Российской Федерации.

На региональном уровне координацию деятельности в области защиты информации осуществляют комиссии по информационной безопасности при руководителе высшего исполнительного органа субъекта Российской Федерации во взаимодействии с территориальными органами уполномоченных федеральных органов исполнительной власти. Положение о комиссии по информационной безопасности при руководителе высшего исполнительного органа субъекта Российской Федерации разрабатывается в соответствии с типовым положением, утвержденным Правительством Российской Федерации. Положение о комиссии утверждается руководителем высшего исполнительного органа субъекта Российской Федерации.

На ведомственном и объектовом уровнях защита информации организуется в рамках функционирования системы организации и управления защитой информации, создаваемой органом, организацией в соответствии с настоящим Положением.

Состав и функции системы организации и управления защитой информации органа, организации определяются в положении по организации защиты информации в органе, организации, разрабатываемом в соответствии с настоящим Положением.

17. Государственная система защита информации функционирует во взаимодействии с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, созданной в соответствии с Указом Президента Российской Федерации от 15 января 2013 г. № 31с.

III. Организация защиты информации в органе, организации

18. Органом, организацией принимаются организационные и технические меры по защите информации с целью:

предотвращения ущерба (рисков) обладателям информации вследствие нарушения ее безопасности;

создания условий для формирования безопасной среды обработки информации.

Для обеспечения безопасности информации ограниченного доступа принимаемые организационные и технические меры должны обеспечивать ее конфиденциальность, целостность и доступность. Для обеспечения безопасности общедоступной информации принимаемые организационные и технические меры должны обеспечивать ее целостность и доступность.

Принимаемые в органе, организации организационные и технические меры по защите информации должны быть взаимоувязанны с иными мерами по обеспечению информационной безопасности органа, организации, в том числе по обнаружению, предупреждению и ликвидации последствий компьютерных атак, реагированию на компьютерные инциденты.

19. Руководитель органа, организации создает систему организации и управления защитой информации и контролирует ее функционирование.

20. Создаваемая в органе, организации система организации и управления защитой информации должна обеспечивать:

определение недопустимых событий (последствий) в органе, организации, наступление которых может привести к ущербу (рискам) для обладателя информации;

выявление, оценку и блокирование угроз безопасности информации;

предотвращение несанкционированного доступа к информации, к объектам информационной инфраструктуры, обрабатывающим информацию, своевременное обнаружение фактов такого несанкционированного доступа;

недопущение воздействия на информацию, объекты информационной инфраструктуры, в результате которого нарушается безопасность обрабатываемой информации;

обеспечение возможности восстановления информации, модифицированной или уничтоженной вследствие несанкционированного доступа (воздействия) к ней и(или) объектам информационной инфраструктуры, обрабатывающим информацию;

организацию и обеспечение безопасности информации с использованием шифровальных (криптографических) средств в случае, когда

их применение необходимо для противодействия угрозам безопасности информации;

повышение уровня знаний работников органа, организации в области защиты информации;

контроль обеспечения защиты информации в органе, организации;

взаимодействие с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации.

21. Защиту информации в органе организует заместитель руководителя органа, на которого возложены полномочия по обеспечению информационной безопасности в органе в соответствии с Указом Президента Российской Федерации от 1 мая 2022 г. № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации» (далее - ответственное лицо). В организации защиту информации организует непосредственно руководитель организации или уполномоченное им лицо.

Обязанности ответственного (уполномоченного) лица включаются в должностной регламент (должностную инструкцию), разрабатываемый с учетом особенностей деятельности органа, организации на основе типового положения о заместителе руководителя органа (организации), ответственного за обеспечение информационной безопасности в органе (организации), утвержденного Правительством Российской Федерации.

22. Разработка и реализация организационных и технических мер по защите информации в органе осуществляются структурным подразделением, на которое возложены функции по обеспечению информационной безопасности органа, организации в соответствии с Указом Президента Российской Федерации от 1 мая 2022 г. № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации» (далее — структурное подразделение).

В случае разработки и осуществления мероприятий по организации и обеспечению безопасности информации с использованием шифровальных (криптографических) средств защиты информации, в органе создается (определяется) подразделение по криптографической защите информации (далее — орган криптографической защиты). Орган криптографической защиты может функционировать в составе структурного подразделения.

В органе местного самоуправления, организации в зависимости от объема работ по защите информации создается (определяется) подразделение по защите информации, выполняющее в том числе функции органа криптографической защиты (при необходимости), или назначаются отдельные

специалисты, на которых возлагаются функции по защите информации, включая функции органа криптографической защиты (при необходимости).

Функции структурного подразделения включаются в положение о структурном подразделении, разрабатываемое с учетом особенностей деятельности органа, организации на основе типового положения о структурном подразделении органа, организации, обеспечивающем информационную безопасность, утвержденного Правительством Российской Федерации.

Структурное подразделение (специалисты) разрабатывает и реализует меры по защите информации во взаимодействии с подразделениями (работниками), эксплуатирующими объекты информационной инфраструктуры, и подразделениями (работниками), обеспечивающими функционирование объектов информационной инфраструктуры.

Специалисты структурного подразделения должны обладать знаниями и умениями в области защиты информации, необходимыми для выполнения возложенных на них функций по защите информации.

23. Для выполнения отдельных работ по защите информации органами, организациями могут привлекаться организации, имеющие лицензии, выданные уполномоченными федеральными органами исполнительной власти в соответствии с Федеральным законом «О лицензировании отдельных видов деятельности».

24. Для обеспечения защиты информации должны применяться средства защиты информации, сертифицированные на соответствие требованиям по безопасности информации, установленным уполномоченными федеральными органами исполнительной власти в пределах полномочий.

Выбор средств защиты информации осуществляется в соответствии с требованиями по безопасности информации, установленными уполномоченными федеральными органами исполнительной власти в пределах их полномочий.

Средства защиты информации должны применяться в соответствии с инструкциями (правилами) по их эксплуатации.

Применяемые средства защиты информации должны быть обеспечены технической поддержкой (поддержкой безопасности) со стороны их разработчиков.

25. Объекты информатизации должны быть аттестованы на соответствие требованиям о защите информации в порядке, установленном Федеральной службой по техническому и экспортному контролю.

Не допускается ввод в эксплуатацию объектов информатизации без аттестата соответствия требованиям о защите информации.

26. Порядок организации и управления защитой информации в органе, организации определяются в положении по организации защиты информации в органе, организации, утверждаемом руководителем органа, организации или уполномоченным им лицом.

Требования к порядку разработки и содержанию положения по организации защиты информации в органе, организации утверждаются Федеральной службой по техническому и экспортному контролю по согласованию с Федеральной службой безопасности Российской Федерации.

Положение по организации защиты информации в органе подлежит согласованию с Федеральной службой по техническому и экспортному контролю и должно учитывать настоящее Положение. В случае организации и обеспечения безопасности информации в органе с использованием шифровальных (криптографических) средств защиты информации, положение по организации защиты информации подлежит согласованию с Федеральной службой безопасности Российской Федерации.

27. Организационные и технические меры по защите информации принимаются в органе, организации в соответствии с ежегодным планом мероприятий по защите информации в органе, организации, утверждаемым руководителем органа, организации или уполномоченным им лицом.

Требования к порядку разработки, содержанию и форме плана утверждаются Федеральной службой по техническому и экспортному контролю по согласованию с Федеральной службой безопасности Российской Федерации.

План мероприятий разрабатывается структурным подразделением (в части мероприятий по организации и обеспечению безопасности информации с использованием шифровальных (криптографических) средств защиты информации — органом криптографической защиты) с участием подразделений (работников), эксплуатирующих объекты информационной инфраструктуры, и подразделений (работников), обеспечивающих функционирование объектов информационной инфраструктуры.

28. По результатам выполнения плана мероприятий по защите информации в органе, организации структурным подразделением (органом криптографической защиты в части мероприятий по организации и обеспечению безопасности информации с использованием шифровальных (криптографических) средств защиты информации) составляется отчет о его выполнении, который подписывается ответственным лицом и представляется руководителю органа, организации для принятия решения о необходимости совершенствования системы организации и управления защитой информации в органе, организации.

Отчет о выполнении плана мероприятий по защите информации в органе после его доклада руководителю органа представляется в Федеральную службу по техническому и экспортному контролю (ее территориальные органы), а в части мероприятий по организации и обеспечению безопасности информации с использованием шифровальных (криптографических) средств защиты информации в соответствующий территориальный орган безопасности.

IV. Контроль обеспечения защиты информации

29. Контроль обеспечения защиты информации проводится в органах, организациях с целью своевременного выявления и предотвращения:

ущерба (рисков) обладателям информации вследствие нарушения ее безопасности;

нарушения условий для формирования безопасной среды обработки информации.

30. Контроль обеспечения защиты информации должен предусматривать проверку выполнения требований о защите информации, а также оценку эффективности принимаемых организационных и технических мер по защите информации.

31. Контроль обеспечения защиты информации осуществляется на межведомственном, ведомственном и объектовом уровнях.

32. На межведомственном уровне контроль обеспечения защиты информации организуется и осуществляется уполномоченными федеральными органами исполнительной власти в пределах их полномочий в порядке, определяемом указанными уполномоченными федеральными органами исполнительной власти.

Органами, организациями обеспечивается беспрепятственный доступ должностных лиц уполномоченных федеральных органов исполнительной власти к информации и объектам информационной инфраструктуры при реализации этими лицами полномочий по осуществлению контроля обеспечения защиты информации.

33. Федеральная служба по техническому и экспортному контролю, в том числе на основе результатов контроля обеспечения защиты информации, осуществляет оценку состояния защиты информации в Российской Федерации (за исключением безопасности информации с использованием шифровальных (криптографических) средств защиты информации) в целях выработки мер по повышению защищенности информации в органах, организациях. Методика такой оценки утверждается Федеральной службой по техническому и

экспортному контролю по согласованию с аппаратом Совета Безопасности Российской Федерации. Результаты оценки ежегодно представляются Секретарю Совета Безопасности Российской Федерации в целях подготовки доклада Президенту Российской Федерации о состоянии национальной безопасности и мерах по ее укреплению.

Оценка состояния защиты информации в Российской Федерации, организуемой и осуществляемой с использованием шифровальных (криптографических) средств защиты информации, проводится Федеральной службой безопасности Российской Федерации в установленном ею порядке.

34. Контроль обеспечения защиты информации на ведомственном уровне организуется и осуществляется органами, в том числе в отношении подведомственных этим органам организаций.

Контроль обеспечения защиты информации на ведомственном уровне организуется и проводится структурным подразделением органа, а в части мероприятий по организации и обеспечению безопасности информации с использованием шифровальных (криптографических) средств защиты информации — органом криптографической защиты органа.

Порядок организации и осуществления ведомственного контроля обеспечения защиты информации на ведомственном уровне определяется руководителем органа в положении об организации защиты информации в органе, разрабатываемом в соответствии с настоящим Положением.

По результатам ведомственного контроля обеспечения защиты информации руководителем органа в случае необходимости принимаются меры по совершенствованию системы организации и управления защитой информации и повышению защищенности информации и объектов информационной инфраструктуры.

35. Контроль обеспечения защиты информации на объектовом уровне осуществляется структурным подразделением организации, а в части мероприятий по организации и обеспечению безопасности информации с использованием шифровальных (криптографических) средств защиты информации — органом криптографической защиты организации.

По результатам контроля разрабатывается отчет о состоянии защиты информации в организации, который утверждается ответственным лицом и представляется руководителю организации для принятия решения о необходимости принятия мер по совершенствованию системы организации и управления защитой информации и повышению защищенности информации и объектов информационной инфраструктуры.

36. Организации проходят независимую оценку защищенности информации и объектов информационной инфраструктуры, обрабатывающих

информацию, с привлечением внешней организации, имеющей лицензии, выданные уполномоченными федеральными органами исполнительной власти в соответствии с Федеральным законом «О лицензировании отдельных видов деятельности».

Порядок организации и проведения, периодичность независимой оценки защищенности информации и объектов информационной инфраструктуры устанавливается Правительством Российской Федерации.