

ПАМЯТКА

**по защите информации, не составляющей государственную тайну,
содержащейся в государственных информационных системах
и в муниципальных информационных системах,
если иное не установлено законодательством
Российской Федерации о местном самоуправлении**

В информационной системе объектами защиты являются информация, содержащаяся в информационной системе, технические средства (в том числе средства вычислительной техники, машинные носители информации, средства и системы связи и передачи данных, технические средства обработки буквенно-цифровой, графической, видео- и речевой информации), общесистемное, прикладное, специальное программное обеспечение, информационные технологии, а также средства защиты информации.

1. Для обеспечения защиты информации, содержащейся в информационной системе, в органе власти назначается структурное подразделение или должностное лицо (работник), ответственные за защиту информации.

2. Мероприятия по обеспечению защиты информации, содержащейся в информационной системе.

2.1. Формирование требований к защите информации, содержащейся в информационной системе:

принятие решения о необходимости защиты информации, содержащейся в информационной системе;

классификация информационной системы по требованиям защиты информации (далее - классификация информационной системы);

определение угроз безопасности информации, реализация которых может привести к нарушению безопасности информации в информационной системе, и разработку на их основе модели угроз безопасности информации;

определение требований к системе защиты информации информационной системы.

2.2. Разработка системы защиты информации информационной системы:

проектирование системы защиты информации информационной системы;

разработка эксплуатационной документации на систему защиты информации информационной системы;

макетирование и тестирование системы защиты информации информационной системы (при необходимости).

2.3. Внедрение системы защиты информации информационной системы:

установка и настройка средств защиты информации в информационной системе;

разработка документов, определяющих правила и процедуры, реализуемые оператором для обеспечения защиты информации в информационной системе в ходе ее эксплуатации (организационно-распорядительные документы по защите информации);

внедрение организационных мер защиты информации;

предварительные испытания системы защиты информации информационной системы;

опытная эксплуатация системы защиты информации информационной системы;

анализ уязвимостей информационной системы и принятие мер защиты информации по их устранению;

приемочные испытания системы защиты информации информационной системы.

2.4. Аттестация информационной системы по требованиям защиты информации (аттестация информационной системы) и ввод ее в действие:

проведение комплекса организационных и технических мероприятий (аттестационных испытаний), в результате которых подтверждается соответствие системы защиты информации информационной системы установленным требованиям;

повторная аттестация информационной системы осуществляется в случае окончания срока действия аттестата соответствия или повышения класса защищенности информационной системы.

2.5. Обеспечение защиты информации в ходе эксплуатации аттестованной информационной системы осуществляется оператором в соответствии с эксплуатационной документацией на систему защиты информации и организационно-распорядительными документами по защите информации и в том числе включает в себя:

управление (администрирование) системой защиты информации информационной системы;

выявление инцидентов и реагирование на них;

управление конфигурацией аттестованной информационной системы и ее системы защиты информации;

контроль (мониторинг) за обеспечением уровня защищенности информации, содержащейся в информационной системе.

2.6. Обеспечение защиты информации при выводе из эксплуатации аттестованной информационной системы или после принятия решения об окончании обработки информации включает в себя:

архивирование информации, содержащейся в информационной системе;

уничтожение (стирание) данных и остаточной информации с машинных носителей информации и (или) уничтожение машинных носителей информации.