

ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ

ПРИКАЗ

от 18 марта 2025 года № 117

Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений, с использованием шифровальных (криптографических) средств

В соответствии с пунктом "ш" части первой статьи 13 Федерального закона от 3 апреля 1995 г. № 40-ФЗ "О федеральной службе безопасности", частью 5 статьи 16 Федерального закона от 27 июля 2006 г. № 149-ФЗ "Об информации, информационных технологиях и о защите информации" и пунктом 1 Положения о Федеральной службе безопасности Российской Федерации, утвержденного Указом Президента Российской Федерации от 11 августа 2003 г. № 960,

приказываю:

1. Утвердить прилагаемые Требования о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений, с использованием шифровальных (криптографических) средств.

2. Установить, что настоящий приказ не распространяется на информационные системы Администрации Президента Российской Федерации, Совета Безопасности Российской Федерации, Федерального Собрания Российской Федерации, Правительства Российской Федерации, Конституционного Суда Российской Федерации, Верховного Суда Российской Федерации и Федеральной службы безопасности Российской Федерации, а также на информационные системы, содержащие сведения, составляющие государственную тайну.

3. Признать утратившим силу приказ ФСБ России от 24 октября 2022 г. № 524 "Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, с использованием шифровальных (криптографических) средств"¹.

¹ Зарегистрирован Минюстом России 23 ноября 2022 г., регистрационный № 71073.

Директор
А.Бортников

Зарегистрировано
в Министерстве юстиции
Российской Федерации
26 марта 2025 года,
регистрационный № 81647

УТВЕРЖДЕНЫ
приказом ФСБ России
от 18 марта 2025 года № 117

Требования о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений, с использованием шифровальных (криптографических) средств

1. Информация, содержащаяся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений¹, подлежит защите с использованием шифровальных (криптографических) средств защиты информации² в случаях, если:

¹ Далее - ИС.

² Далее-СКЗИ.

законодательными и (или) иными нормативными правовыми актами Российской Федерации предусмотрена обязанность по защите информации, содержащейся в ИС, с использованием СКЗИ;

в ИС осуществляется передача информации по каналам связи, проходящим за периметром охраняемой территории предприятия (учреждения), ограждающих конструкций охраняемого здания, охраняемой части здания, выделенного помещения³;

³ Далее - контролируемая зона.

необходимо признание электронных документов, подписанных электронной подписью, равнозначными документам на бумажном носителе, подписанным собственноручной подписью;

в ИС осуществляется хранение данных на носителях информации, предназначенных для записи, хранения и воспроизведения информации, обрабатываемой с использованием средств вычислительной техники, несанкционированный доступ к которым со стороны третьих лиц не может быть исключен с помощью некриптографических методов и способов.

2. Необходимость использования СКЗИ для защиты информации, содержащейся в ИС, подлежит обоснованию в модели угроз безопасности информации, техническом проекте и техническом задании на создание (развитие) ИС.

Модель угроз безопасности информации и (или) техническое задание на создание (развитие) государственных информационных систем подлежат согласованию с ФСБ России в части криптографической защиты информации¹.

¹ Абзац второй пункта 3 требований к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем и дальнейшего хранения содержащейся в их базах данных информации, утвержденных постановлением Правительства Российской Федерации от 6 июля 2015 г. № 676.

3. Для обеспечения защиты информации, содержащейся в ИС, должны использоваться СКЗИ, сертифицированные ФСБ России².

² Подпункт 21 пункта 9 Положения о Федеральной службе безопасности Российской Федерации, утвержденного Указом Президента Российской Федерации от 11 августа 2003 г. № 960.

4. Для противодействия угрозам безопасности информации с использованием аппаратных, программно-аппаратных и (или) программных средств, направленным на нарушение безопасности защищаемой СКЗИ информации либо на создание условий для этого³, должны использоваться СКЗИ класса, определенного в соответствии с пунктами 7-18 настоящих Требований.

³ Далее - атаки.

Класс СКЗИ, определенный в соответствии с пунктами 7-18 настоящих Требований, подлежит обоснованию в модели угроз безопасности информации.

5. В случае если это предусмотрено документацией на СКЗИ в отношении аппаратных, программно-аппаратных и программных средств, с которыми в ИС предполагается штатное функционирование СКЗИ⁴, должна быть проведена оценка их влияния на выполнение предъявляемых к СКЗИ требований¹.

⁴Далее - технические средства.

¹Далее - оценка влияния среды функционирования.

Оценка влияния среды функционирования проводится организацией, уполномоченной на осуществление криптографических, инженерно-криптографических и специальных исследований СКЗИ (тематических исследований СКЗИ) в соответствии с Положением о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005), утвержденным приказом ФСБ России от 9 февраля 2005 г. № 66 ².

² Зарегистрирован Минюстом России 3 марта 2005 г., регистрационный № 6382 (с изменениями, внесенными приказом ФСБ России от 12 апреля 2010 г. № 173, зарегистрирован Минюстом России 25 мая 2010 г., регистрационный № 17350).

Результаты оценки влияния среды функционирования, образцы СКЗИ, которые планируется использовать для защиты информации, содержащейся в ИС, и технических средств должны пройти экспертизу в ФСБ России³.

³ Пункт 33 Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005), утвержденного приказом ФСБ России от 9 февраля 2005 г. № 66.

Обработка защищаемой информации в ИС при использовании для ее защиты СКЗИ совместно с иными техническими средствами допускается при наличии положительного заключения ФСБ России, подготовленного по результатам экспертизы.

6. В помещениях, в которых размещены и (или) хранятся СКЗИ и (или) носители ключевой, аутентифицирующей и парольной информации СКЗИ, должен обеспечиваться режим, препятствующий возможности неконтролируемого проникновения или пребывания лиц, не имеющих права доступа в такие помещения, который достигается посредством:

утверждения правил доступа в помещения в рабочее и нерабочее время, а также в нештатных ситуациях;

утверждения перечня лиц, имеющих право доступа в помещения.

Помещения, в которых размещены и (или) хранятся СКЗИ и (или) носители ключевой, аутентифицирующей и парольной информации СКЗИ, предназначенные для защиты информации, содержащейся в ИС или составной части ИС¹, предназначенной для решения задач ИС на всей территории Российской Федерации или в пределах двух и более субъектов Российской Федерации, обрабатывающей информацию высокого уровня значимости, должны соответствовать следующим требованиям:

¹Далее - сегмент ИС.

окна помещений, расположенных на первых и (или) последних этажах зданий, а также окна помещений, находящихся около пожарных лестниц и других мест, откуда возможно проникновение в помещения посторонних лиц, должны быть оборудованы металлическими решетками или ставнями, охранной сигнализацией или другими средствами, препятствующими неконтролируемому проникновению посторонних лиц в помещения;

окна и двери помещений, в которых размещены серверы ИС, должны быть оборудованы металлическими решетками, охранной сигнализацией или другими средствами, препятствующими неконтролируемому проникновению посторонних лиц в помещения.

7. Класс СКЗИ, подлежащих использованию для защиты информации, содержащейся в ИС, определяется для каждого сегмента ИС, предназначенного для решения задач ИС в пределах определенной территории или объекта (объектов).

В случае если ИС не содержит сегментов ИС, то класс СКЗИ, необходимый для защиты содержащейся в ней информации, определяется для ИС в целом.

8. Определение класса СКЗИ, подлежащих использованию для защиты информации, содержащейся в ИС, осуществляется в зависимости от уровня значимости обрабатываемой в ИС информации и масштаба ИС в соответствии с таблицей, приведенной в приложении к настоящим Требованиям, и особенностями, предусмотренными пунктами 10-18 настоящих Требований.

Уровень значимости информации, содержащейся в ИС, определяется обладателем информации (заказчиком) и (или) оператором в зависимости от нарушения конфиденциальности (неправомерные доступ, копирование, предоставление или распространение), целостности (неправомерные уничтожение или модификация) или доступности (неправомерное блокирование) информации¹.

¹ Далее - свойства безопасности информации.

Информация имеет высокий уровень значимости, если в результате нарушения хотя бы одного из свойств безопасности информации ИС и (или) оператор, обладатель информации не могут выполнять возложенные на них функции.

Информация имеет средний уровень значимости, если в результате нарушения хотя бы одного из свойств безопасности информации ИС и (или) оператор, обладатель информации не могут выполнять хотя бы одну из возложенных на них функций.

Информация имеет низкий уровень значимости, если в результате нарушения хотя бы одного из свойств безопасности информации ИС и (или) оператор, обладатель информации могут выполнять возложенные на них функции только с привлечением дополнительных сил и средств.

9. В случае если ИС состоит из двух и более сегментов ИС, то уровень значимости информации и масштаб определяются для каждого сегмента ИС отдельно.

10. Класс СКЗИ, подлежащих использованию для защиты информации в ИС (сегменте ИС), при ее взаимодействии с другими ИС и (или) сегментами других ИС определяется по более высокому классу СКЗИ, используемому для защиты информации во взаимодействующих ИС и (или) сегментах ИС.

11. Класс СКЗИ, подлежащих использованию для защиты информации во взаимодействующих между собой сегментах одной ИС, определяется не ниже наименьшего класса СКЗИ, используемого для защиты информации в таких сегментах ИС.

12. В случае если в модели угроз безопасности информации в качестве актуальной угрозы определена возможность источника атак самостоятельно осуществлять создание способов атак, подготовку и проведение атак только вне пределов контролируемой зоны, то для защиты информации в ИС (сегменте ИС) необходимо использовать СКЗИ класса КС1.

13. В случае если в модели угроз безопасности информации в качестве актуальной угрозы определена возможность источника атак самостоятельно осуществлять создание способов атак, подготовку и проведение атак в пределах контролируемой зоны, но без физического доступа к аппаратным средствам, на которых реализованы СКЗИ и среда их функционирования, то для защиты информации в ИС (сегменте ИС) необходимо использовать СКЗИ класса КС2.

Правило, указанное в абзаце первом настоящего пункта, применяется, если для защиты информации, содержащейся в ИС (сегменте ИС), в соответствии с таблицей, приведенной в приложении к настоящим Требованиям, необходимо использовать СКЗИ класса КС1.

14. В случае если в модели угроз безопасности информации в качестве актуальной угрозы определена возможность источника атак самостоятельно осуществлять создание способов атак, подготовку и проведение атак в пределах контролируемой зоны с физическим доступом к аппаратным средствам, на которых реализованы СКЗИ и среда их функционирования, то для защиты информации в ИС (сегменте ИС) необходимо использовать СКЗИ класса КС3.

Правило, указанное в абзаце первом настоящего пункта, применяется, если для защиты информации, содержащейся в ИС (сегменте ИС), в соответствии с таблицей, приведенной в приложении к настоящим Требованиям, необходимо использовать СКЗИ класса КС1 или КС2.

15. В случае если в модели угроз безопасности информации в качестве актуальной угрозы определена возможность источника атак привлекать специалистов, имеющих опыт разработки и анализа СКЗИ, включая специалистов в области анализа сигналов линейной передачи и сигналов побочного электромагнитного излучения и наводок СКЗИ и специалистов в области использования для реализации атак недокументированных возможностей прикладного программного обеспечения, то для защиты информации в ИС (сегменте ИС) необходимо использовать СКЗИ класса КВ.

Правило, указанное в абзаце первом настоящего пункта, применяется, если для защиты информации, содержащейся в ИС (сегменте ИС), в соответствии с таблицей, приведенной в приложении к настоящим Требованиям, необходимо использовать СКЗИ класса КС1, КС2 или КС3.

16. В случае если в модели угроз безопасности информации в качестве актуальной угрозы определена возможность источника атак привлекать специалистов, имеющих опыт разработки и анализа СКЗИ, включая специалистов в области использования для реализации атак недокументированных возможностей аппаратного и программного компонентов среды функционирования СКЗИ, то для защиты информации в ИС (сегменте ИС) необходимо использовать СКЗИ класса КА.

17. Класс СКЗИ, используемых для взаимодействия граждан (физических лиц) с ИС (сегментом ИС), определяется исходя из актуальных угроз безопасности информации и может быть ниже класса СКЗИ, определенного для ИС (сегмента ИС) в соответствии с настоящими Требованиями.

18. В случае если иными нормативными правовыми актами, устанавливающими требования о защите информации с использованием СКЗИ, предусмотрена необходимость использовать для защиты информации СКЗИ более высокого класса, чем класс СКЗИ, определенный в соответствии с настоящими Требованиями, то класс СКЗИ, подлежащих использованию в ИС (сегменте ИС), определяется в соответствии с такими нормативными правовыми актами.

Приложение
к Требованиям (пункты 8, 13-15)

**Таблица определения минимально допустимого класса СКЗИ, подлежащих использованию
для защиты информации, содержащейся в ИС (сегменте ИС)**

Уровень значимости информации	Масштаб ИС (сегмента ИС)		
	ИС (сегмент ИС), предназначенная для решения задач ИС на всей территории Российской Федерации или в пределах двух и более субъектов Российской Федерации	ИС (сегмент ИС), предназначенная для решения задач ИС в пределах одного субъекта Российской Федерации	ИС (сегмент ИС), предназначенная для решения задач ИС в пределах объекта (объектов) одного государственного органа, муниципального образования и (или) организации
Высокий уровень значимости	КВ	КС3	КС2

Средний уровень значимости	KC3	KC3	KC1
Низкий уровень значимости	KC2	KC1	KC1