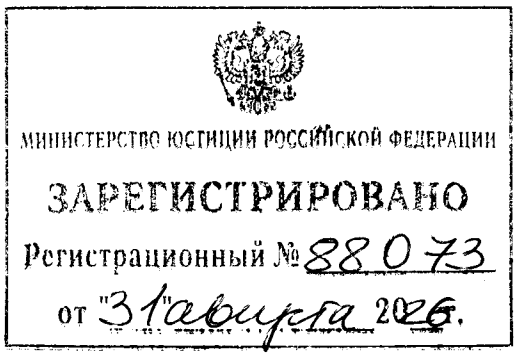
ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ

ПРИКАЗ

22 августа 2026 года Москва № 321



Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений, а также при использовании технических средств и программ для электронных вычислительных машин и баз данных в соответствии с частью 5^1 статьи 13 Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» 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,

П Р И К А З Ы В А Ю:

1. Утвердить прилагаемые Требования о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений, а также при использовании технических средств и программ для электронных вычислительных машин и баз данных в соответствии с частью 5[1] статьи 13 Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» 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 18 марта 2025 г. № 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»[1].

Директор А.Бортников

[1] Зарегистрирован Минюстом России 26 марта 2025 г., регистрационный № 81647.

Утверждены
приказом ФСБ России
от 22 августа 2026г.
№ 321

Требования
о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений, а также при использовании технических средств и программ для электронных вычислительных машин и баз данных в соответствии с частью 5[1] статьи 13 Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» с использованием шифровальных (криптографических) средств

1. Информация, содержащаяся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений[1], а также обрабатываемая при использовании технических средств и программ для электронных вычислительных машин и баз данных в соответствии с частью 5[1] статьи 13 Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»[2], подлежит защите с использованием шифровальных (криптографических) средств[3] в случаях, если:

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

в ИС, а также при использовании технических средств и программ для электронных вычислительных машин и баз данных в соответствии с частью 5[1] статьи 13 Федерального закона осуществляется передача информации по каналам связи, проходящим за периметром охраняемой

[1] Далее – ИС.
[2] Далее – Федеральный закон.
[3] Далее – СКЗИ.

территории, ограждающих конструкций охраняемого здания, охраняемой части здания, выделенного помещения[1];

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

в ИС осуществляется передача информации по каналам связи, проходящим в пределах контролируемой зоны, а также хранение данных на носителях информации, предназначенных для записи, хранения и воспроизведения информации, обрабатываемой с использованием электронных вычислительных машин, 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 и (или) 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 информации[2].

3. Для обеспечения защиты информации, содержащейся в ИС, а также при использовании технических средств и программ для электронных вычислительных машин и баз данных в соответствии с частью 5^1 статьи 13 Федерального закона должны использоваться СКЗИ, сертифицированные ФСБ России[3].

Ввод СКЗИ в эксплуатацию должен осуществляться на основании акта, подтверждающего выполнение требований эксплуатационной и технической документации на СКЗИ, а также требований нормативных правовых актов

---

[1] Далее – контролируемая зона.

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

Российской Федерации в области обеспечения защиты информации с использованием СКЗИ.

Смена ключевой информации должна осуществляться в соответствии с эксплуатационной и технической документацией на СКЗИ.

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 этого[1], должны использоваться СКЗИ класса, определенного в соответствии с пунктами 7 – 17 настоящих Требований.

Класс СКЗИ, определенный в соответствии с пунктами 7 – 17 настоящих Требований, подлежит обоснованию в модели угроз безопасности информации.

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

Оценка влияния, предусмотренная абзацем первым настоящего пункта, проводится организацией, уполномоченной на осуществление криптографических, инженерно-криптографических и специальных 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].

6. В помещениях, в которых размещены и (или) хранятся СКЗИ и (или) носители ключевой, аутентифицирующей и парольной информации СКЗИ, должен обеспечиваться режим, препятствующий возможности

---

[1] Далее – атаки.

[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).

неконтролируемого проникновения или пребывания лиц, не имеющих права доступа в такие помещения[1], который достигается посредством утверждения:

схемы криптографической защиты, разработанной на основании модели угроз безопасности информации, с указанием актуальных сведений о помещениях, указанных в абзаце первом настоящего пункта, о каналах связи, подлежащих защите с использованием СКЗИ, а также с указанием наименований и класса применяемых СКЗИ;

правил доступа в помещения, указанные в абзаце первом настоящего пункта, в рабочее и нерабочее время, а также в нештатных ситуациях;

перечня лиц, имеющих право доступа в помещения, указанные в абзаце первом настоящего пункта.

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 ИС[2], 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:

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.

---

[1] Далее – посторонние лица.

[2] Далее – сегмент ИС.

Размещение СКЗИ, в том числе при использовании технических средств и программ для электронных вычислительных машин и баз данных в соответствии с частью 5^1 статьи 13 Федерального закона, в помещениях, в которые имеют доступ лица, не допущенные к СКЗИ, должно препятствовать неконтролируемому доступу к СКЗИ, в том числе путем опечатывания (опломбирования) стоек, в которых они установлены. При этом факты вскрытия и опечатывания (опломбирования) стоек должны фиксироваться документально с указанием номера стойки, даты и времени ее вскрытия и опечатывания (опломбирования), проведенных действий, фамилии, имени, отчества (при наличии) лица, проводившего вскрытие и опечатывание (опломбирование), и проставлением им подписи.

7. Класс СКЗИ, подлежащих использованию для защиты информации, содержащейся в ИС, определяется для ИС в целом.

Класс СКЗИ, подлежащих использованию для защиты информации, содержащейся в ИС, состоящей из сегментов ИС, определяется для ИС в целом или для каждого сегмента ИС отдельно.

При использовании в соответствии с частью 5^1 статьи 13 Федерального закона для обеспечения создания и эксплуатации государственных информационных систем, иных информационных систем государственных органов, технических средств, программ для электронных вычислительных машин и баз данных, доступ к которым предоставляется с использованием информационно-телекоммуникационных сетей, необходимо использовать СКЗИ определенного для указанных информационных систем класса.

8. Определение минимально допустимого класса СКЗИ, подлежащих использованию для защиты информации, содержащейся в ИС (сегменте ИС), осуществляется в зависимости от уровня значимости информации, содержащейся в ИС (сегменте ИС), и масштаба ИС (сегмента ИС) в соответствии с таблицей, приведенной в приложении к настоящим Требованиям, и особенностями, предусмотренными пунктами 9 – 17 настоящих Требований.

Уровень значимости информации, содержащейся в ИС (сегменте ИС), определяется обладателем информации (заказчиком) и (или) оператором ИС

в зависимости от степени возможного ущерба от нарушения конфиденциальности (неправомерные доступ, копирование, предоставление или распространение), целостности (неправомерное уничтожение или модифицирование) или доступности (неправомерное блокирование) информации[1].

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

9. Класс СКЗИ, подлежащих использованию для защиты информации в ИС (сегменте ИС), при ее взаимодействии с другими информационными системами и (или) сегментами других информационных систем определяется по наиболее высокому классу СКЗИ, используемому для защиты информации во взаимодействующих информационных системах и (или) сегментах информационных систем.

10. В отношении ИС, состоящей из сегментов ИС, для каждого из которых определен класс СКЗИ, класс СКЗИ, подлежащих использованию для защиты информации во взаимодействующих между собой сегментах ИС такой ИС, определяется не ниже наименьшего класса СКЗИ, используемого для защиты информации в таких сегментах ИС.

11. 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

---

[1] Далее – свойства безопасности информации.

вне пределов контролируемой зоны, то для защиты информации в ИС (сегменте ИС) необходимо использовать СКЗИ класса КС1 и выше.

12. В случае если в соответствии с таблицей, приведенной в приложении к настоящим Требованиям, необходимо использовать СКЗИ класса КС1, а 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 и выше.

13. В случае если в соответствии с таблицей, приведенной в приложении к настоящим Требованиям, необходимо использовать СКЗИ класса КС1 или КС2, а 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 и выше.

14. В случае если в соответствии с таблицей, приведенной в приложении к настоящим Требованиям, необходимо использовать СКЗИ класса КС1, КС2 или КС3, а 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 и выше.

15. В случае если в соответствии с таблицей, приведенной в приложении к настоящим Требованиям, необходимо использовать СКЗИ класса КС1, КС2, КС3 или КВ, а 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.

16. 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.

17. В случае если иными нормативными правовыми актами, устанавливающими требования о защите информации с использованием СКЗИ, предусмотрена необходимость использования 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.

18. Требования, предусмотренные пунктами 2 – 17 настоящих Требований, должны быть проверяемыми в ходе осуществления внутреннего контроля, организуемого оператором ИС самостоятельно и (или) с привлечением юридических лиц и индивидуальных предпринимателей, имеющих лицензию на осуществление деятельности, предусмотренной пунктом 1 части 1 статьи 12 Федерального закона от 4 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности», не реже одного раза в 3 года.

Приложение
к Требованиям (пункты 8, 12 – 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 одного муниципального образования или объекта (объектов) одного государственного органа, государственного унитарного предприятия или государственного учреждения
Высокий уровень значимости	КВ	КС3	КС2
Средний уровень значимости	КС3	КС3	КС1
Низкий уровень значимости	КС2	КС1	КС1