ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ

ПРИКАЗ

24 октября 2022 года Москва № 524

Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, с использованием шифровальных (криптографических) средств

МИНИСТЕРСТВО ЮСТИЦИИ РОССИЙСКОЙ ФЕДЕРАЦИИ
ЗАРЕГИСТРИРОВАНО
Регистрационный № 71073
от "23" ноября 2022 г.

В соответствии с частью 5 статьи 16 Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»[1], пунктом «ш» части 1 статьи 13 Федерального закона от 3 апреля 1995 г. № 40-ФЗ «О федеральной службе безопасности»[2] и пунктом 1 Положения о Федеральной службе безопасности Российской Федерации, утвержденного Указом Президента Российской Федерации от 11 августа 2003 г. № 960[3],

П Р И К А З Ы В А Ю:

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

[1] Собрание законодательства Российской Федерации, 2006, № 31, ст. 3448; 2014, № 30, ст. 4243.
[2] Собрание законодательства Российской Федерации, 1995, № 15, ст. 1269; 2003, № 27, ст. 2700.
[3] Собрание законодательства Российской Федерации, 2003, № 33 ст. 3254; 2007, № 1, ст. 205.

2. Установить, что настоящий приказ не распространяется на государственные 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 государственные информационные системы, содержащие сведения, составляющие государственную тайну.

3. Настоящий приказ вступает в силу по истечении одного года со дня его официального опубликования.

Директор А.Бортников

Утверждены
приказом ФСБ России
от 24 октября 2022г.
№ 524

Требования
о защите информации, содержащейся в государственных информационных системах, с использованием шифровальных (криптографических) средств

I. Защита информации, содержащейся в государственных информационных системах, с использованием шифровальных (криптографических) средств

1. Информация, содержащаяся в государственных информационных системах (далее – ГИС), подлежит защите с использованием шифровальных (криптографических) средств защиты информации (далее – СКЗИ) в случаях, если:

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

в ГИС осуществляется передача информации по каналам связи, проходящим за периметром охраняемой территории предприятия (учреждения), ограждающих конструкций охраняемого здания, охраняемой части здания, выделенного помещения (далее – контролируемая зона);

необходимо обеспечить юридическую значимость электронных документов и защиту их от подделки;

в ГИС 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 ГИС, подлежит обоснованию в модели угроз безопасности

информации, техническом проекте и техническом задании на создание (развитие) ГИС. Модель угроз безопасности информации и (или) техническое задание на создание (развитие) ГИС подлежат согласованию с ФСБ России в части криптографической защиты информации[1].

3. Для обеспечения защиты информации, содержащейся в ГИС, должны использоваться только СКЗИ, сертифицированные ФСБ России.

4. Для противодействия угрозам, представляющим собой целенаправленные действия с использованием аппаратных, программно-аппаратных и (или) программных средств, направленные на нарушение безопасности защищаемой СКЗИ информации либо на создание условий для этого (далее – атаки), должны использоваться СКЗИ соответствующего класса, определенного в соответствии с главой II настоящих Требований.

Класс СКЗИ, определенный в соответствии с главой II 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 ГИС предполагается штатное функционирование СКЗИ (далее – технические средства), должна быть проведена оценка их влияния на выполнение предъявляемых к СКЗИ требований (далее – 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

---

[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 (Собрание законодательства Российской Федерации, 2015, № 28, ст. 4241; 2021, № 23, ст. 4079).

(криптографических) средств защиты информации (Положение ПКЗ-2005), утвержденным приказом ФСБ России от 9 февраля 2005 г. № 66[1].

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

Обработка защищаемой информации в ГИС при использовании для ее защиты СКЗИ совместно с иными техническими средствами допускается только 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 ГИС или составной части ГИС (далее – сегмент ГИС), предназначенной для решения задач ГИС 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,

---

[1] 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).

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 ГИС, должны быть оборудованы металлическими решетками, охранной сигнализацией или другими средствами, препятствующими неконтролируемому проникновению посторонних лиц в помещения.

II. Правила определения класса СКЗИ

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

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

8. Определение класса СКЗИ, подлежащих использованию для защиты информации, содержащейся в ГИС, осуществляется в зависимости от уровня значимости обрабатываемой в ГИС информации и масштаба ГИС в соответствии с таблицей, приведенной в приложении к настоящим Требованиям, с учетом особенностей, предусмотренных пунктами 10 – 18 настоящих Требований.

Уровень значимости информации, содержащейся в ГИС, определяется степенью возможного ущерба для обладателя информации (заказчика) и (или) оператора от нарушения конфиденциальности (неправомерные доступ, копирование, предоставление или распространение), целостности (неправомерные уничтожение или модифицирование) или доступности (неправомерное блокирование) информации (далее – свойства безопасности информации).

Информация имеет высокий уровень значимости, если в результате нарушения хотя бы одного из свойств безопасности информации возможны существенные негативные последствия в социальной, политической, международной, экономической, финансовой или иных областях деятельности и (или) ГИС 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 возможны умеренные негативные последствия в социальной, политической, международной, экономической, финансовой или иных областях деятельности и (или) ГИС 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 возможны незначительные негативные последствия в социальной, политической, международной, экономической, финансовой или иных областях деятельности и (или) ГИС и (или) оператор, обладатель информации могут выполнять возложенные на них функции с недостаточной эффективностью или выполнение функций возможно только с привлечением дополнительных сил и средств.

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

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

11. Класс СКЗИ, подлежащих использованию для защиты информации во взаимодействующих между собой сегментах одной ГИС, определяется не

ниже наименьшего класса СКЗИ, используемого для защиты информации в таких сегментах ГИС.

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

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 только вне пределов контролируемой зоны, то для защиты информации в ГИС (сегменте ГИС), в том числе при взаимодействии граждан (физических лиц) с ГИС (сегментом ГИС), 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, но без физического доступа к аппаратным средствам, на которых реализованы СКЗИ и среда их функционирования, то для защиты информации в ГИС (сегменте ГИС), в том числе при взаимодействии граждан (физических лиц) с ГИС (сегментом ГИС), необходимо использовать СКЗИ класса КС2.

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

15. 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 ГИС (сегменте ГИС), в том числе при

взаимодействии граждан (физических лиц) с ГИС (сегментом ГИС), необходимо использовать СКЗИ класса КС3.

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

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 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 ГИС (сегменте ГИС), в том числе при взаимодействии граждан (физических лиц) с ГИС (сегментом ГИС), необходимо использовать СКЗИ класса КВ.

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

17. 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 ГИС (сегменте ГИС), в том числе при взаимодействии граждан (физических лиц) с ГИС (сегментом ГИС), необходимо использовать СКЗИ класса КА.

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 ГИС (сегменте ГИС), определяется в соответствии с такими нормативными правовыми актами.

Приложение
к Требованиям (пп. 8, 14 – 16)

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

Уровень значимости информации	Масштаб ГИС (сегмента ГИС)		
	ГИС (сегмент ГИС), предназначенная для решения задач ГИС на всей территории Российской Федерации или в пределах двух и более субъектов Российской Федерации	ГИС (сегмент ГИС), предназначенная для решения задач ГИС в пределах одного субъекта Российской Федерации	ГИС (сегмент ГИС), предназначенная для решения задач ГИС в пределах объекта (объектов) одного государственного органа, муниципального образования и (или) организации
Высокий уровень значимости	КВ	КС3	КС2
Средний уровень значимости	КС3	КС3	КС1
Низкий уровень значимости	КС2	КС1	КС1