Утверждены
приказом ФСБ России
от
№

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

I. Защита 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 учреждений[1], подлежит защите с использованием шифровальных (криптографических) средств защиты информации[2] в случаях, если:

законодательными и 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 помещения[3];

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

---

[1] Далее – ИС.
[2] Далее – СКЗИ.
[3] Далее – контролируемая зона.

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 информации[1].

3. Для обеспечения защиты информации, содержащейся в ИС, 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[2], 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

---

[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.

[2] Далее – атаки.

которыми в ИС предполагается штатное функционирование СКЗИ[1], должна быть проведена оценка их влияния на выполнение предъявляемых к СКЗИ требований[2].

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[3].

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

Обработка защищаемой информации в ИС 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,

---

[1] Далее – технические средства.

[2] Далее – оценка влияния среды функционирования.

[3] 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).

предназначенные для защиты информации, содержащейся в ИС или составной части ИС[1], 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.

II. Правила определения класса СКЗИ

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, с учетом особенностей, предусмотренных пунктами 10 – 18 настоящих Требований.

[1] Далее – сегмент ИС.

Уровень значимости информации, содержащейся в ИС, 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[1].

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) 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 возможны умеренные негативные последствия в социальной, политической, международной, экономической, финансовой или иных областях деятельности и (или) 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 возможны незначительные негативные последствия в социальной, политической, международной, экономической, финансовой или иных областях деятельности и (или) ИС 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 ИС состоит из двух и более сегментов ИС, то уровень значимости информации и масштаб определяются для каждого сегмента ИС отдельно.

---

[1] Далее – свойства безопасности информации.

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 с учетом 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.