Приказ ФСБ России от 10 июля 2014 г. № 378
«Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»

В соответствии с **частью 4 статьи 19** Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных»* приказываю:

- утвердить прилагаемые **Состав и содержание** организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации **требований** к защите персональных данных для каждого из уровней защищенности.

Директор А. Бортников

Зарегистрировано в Минюсте РФ 18 августа 2014 г.
Регистрационный № 33620

---

* Собрание законодательства Российской Федерации, 2006, № 31 (ч. I), ст. 3451; 2009, № 48, ст. 5716, № 52 (ч. I), ст. 6439; 2010, № 27, ст. 3407; № 31, ст. 4173, ст. 4196; № 49, ст. 6409; № 52 (ч. 1), ст. 6974; 2011, № 23, ст. 3263; № 31, ст. 4701; 2013, № 14, ст. 1651; № 30 (ч. 1), ст. 4038.

www.alfario.ru

Приложение
к приказу Федеральной
службы безопасности РФ
от 10 июля 2014 г. № 378

Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности

I. Общие положения

1. Настоящий документ определяет состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных (далее - информационная система) с использованием средств криптографической защиты информации (далее - СКЗИ), необходимых для выполнения установленных Правительством Российской Федерации **требований** к защите персональных данных для каждого из уровней защищенности.

2. Настоящий документ предназначен для операторов, использующих СКЗИ для обеспечения безопасности персональных данных при их обработке в информационных системах.

3. Применение организационных и технических мер, определенных в настоящем документе, обеспечивает оператор с учетом требований эксплуатационных документов на СКЗИ, используемые для обеспечения безопасности персональных данных при их обработке в информационных системах.

4. Эксплуатация СКЗИ должна осуществляться в соответствии с документацией на СКЗИ и требованиями, установленными в настоящем документе, а также в соответствии с иными нормативными правовыми актами, регулирующими отношения в соответствующей области.

II. Состав и содержание организационных и технических мер, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для 4 уровня защищенности

5. В соответствии с **пунктом 13** Требований к защите персональных данных при их обработке в информационных системах персональных данных, утвержденных **постановлением** Правительства Российской Федерации от 1 ноября 2012 г. № 1119* (далее - Требования к защите персональных данных), для обеспечения 4 уровня защищенности персональных данных при их обработке в информационных системах необходимо выполнение следующих требований:

а) организация режима обеспечения безопасности помещений, в которых размещена информационная система, препятствующего возможности

www.alfario.ru

неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения;

б) обеспечение сохранности носителей персональных данных;

в) утверждение руководителем оператора документа, определяющего перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей;

г) использование средств защиты информации, прошедших процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз.

6. Для выполнения требования, указанного в **подпункте «а» пункта 5** настоящего документа, необходимо обеспечение режима, препятствующего возможности неконтролируемого проникновения или пребывания в помещениях, где размещены используемые СКЗИ, хранятся СКЗИ и (или) носители ключевой, аутентифицирующей и парольной информации СКЗИ (далее - Помещения), лиц, не имеющих права доступа в Помещения, которое достигается путем:

а) оснащения Помещений входными дверьми с замками, обеспечения постоянного закрытия дверей Помещений на замок и их открытия только для санкционированного прохода, а также опечатывания Помещений по окончании рабочего дня или оборудование Помещений соответствующими техническими устройствами, сигнализирующими о несанкционированном вскрытии Помещений;

б) утверждения правил доступа в Помещения в рабочее и нерабочее время, а также в нештатных ситуациях;

в) утверждения перечня лиц, имеющих право доступа в Помещения.

7. Для выполнения требования, указанного в **подпункте «б» пункта 5** настоящего документа, необходимо:

а) осуществлять хранение съемных машинных носителей персональных данных в сейфах (металлических шкафах), оборудованных внутренними замками с двумя или более дубликатами ключей и приспособлениями для опечатывания замочных скважин или кодовыми замками. В случае если на съемном машинном носителе персональных данных хранятся только персональные данные в зашифрованном с использованием СКЗИ виде, допускается хранение таких носителей вне сейфов (металлических шкафов);

б) осуществлять поэкземплярный учет машинных носителей персональных данных, который достигается путем ведения журнала учета носителей персональных данных с использованием регистрационных (заводских) номеров.

8. Для выполнения требования, указанного в **подпункте «в» пункта 5** настоящего документа, необходимо:

а) разработать и утвердить документ, определяющий перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей;

б) поддерживать в актуальном состоянии документ, определяющий перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей.

9. Для выполнения требования, указанного в **подпункте «г» пункта 5** настоящего документа, необходимо для каждого из уровней защищенности

www.alfario.ru

персональных данных применение СКЗИ соответствующего класса, позволяющих обеспечивать безопасность персональных данных при реализации целенаправленных действий с использованием аппаратных и (или) программных средств с целью нарушения безопасности защищаемых СКЗИ персональных данных или создания условий для этого (далее - атака), которое достигается путем:

а) получения исходных данных для формирования совокупности предположений о возможностях, которые могут использоваться при создании способов, подготовке и проведении атак;

б) формирования и утверждения руководителем оператора совокупности предположений о возможностях, которые могут использоваться при создании способов, подготовке и проведении атак, и определение на этой основе и с учетом типа актуальных угроз требуемого класса СКЗИ;

в) использования для обеспечения требуемого уровня защищенности персональных данных при их обработке в информационной системе СКЗИ класса КС1 и выше.

10. СКЗИ **класса КС1** применяются для нейтрализации атак, при создании способов, подготовке и проведении которых используются возможности из числа следующих:

а) создание способов, подготовка и проведение атак без привлечения специалистов в области разработки и анализа СКЗИ;

б) создание способов, подготовка и проведение атак на различных этапах жизненного цикла СКЗИ**;

в) проведение атаки, находясь вне пространства, в пределах которого осуществляется контроль за пребыванием и действиями лиц и (или) транспортных средств (далее - контролируемая зона)***;

г) проведение на этапах разработки (модернизации), производства, хранения, транспортировки СКЗИ и этапе ввода в эксплуатацию СКЗИ (пусконаладочные работы) следующих атак:

- внесение несанкционированных изменений в СКЗИ и (или) в компоненты аппаратных и программных средств, совместно с которыми штатно функционируют СКЗИ и в совокупности представляющие среду функционирования СКЗИ (далее - СФ), которые способны повлиять на выполнение предъявляемых к СКЗИ требований, в том числе с использованием вредоносных программ;

- внесение несанкционированных изменений в документацию на СКЗИ и компоненты СФ;

д) проведение атак на этапе эксплуатации СКЗИ на:

- персональные данные;

- ключевую, аутентифицирующую и парольную информацию СКЗИ;

- программные компоненты СКЗИ;

- аппаратные компоненты СКЗИ;

- программные компоненты СФ, включая программное обеспечение BIOS;

- аппаратные компоненты СФ;

- данные, передаваемые по каналам связи;

- иные объекты, которые установлены при формировании совокупности предположений о возможностях, которые могут использоваться при создании способов, подготовке и проведении атак с учетом применяемых в информационной

www.alfario.ru

системе информационных технологий, аппаратных средств (далее - АС) и программного обеспечения (далее - ПО);

е) получение из находящихся в свободном доступе источников (включая информационно-телекоммуникационные сети, доступ к которым не ограничен определенным кругом лиц, в том числе информационно-телекоммуникационную сеть «Интернет») информации об информационной системе, в которой используется СКЗИ. При этом может быть получена следующая информация:

- общие сведения об информационной системе, в которой используется СКЗИ (назначение, состав, оператор, объекты, в которых размещены ресурсы информационной системы);

- сведения об информационных технологиях, базах данных, АС, ПО, используемых в информационной системе совместно с СКЗИ, за исключением сведений, содержащихся только в конструкторской документации на информационные технологии, базы данных, АС, ПО, используемые в информационной системе совместно с СКЗИ;

- содержание конструкторской документации на СКЗИ;

- содержание находящейся в свободном доступе документации на аппаратные и программные компоненты СКЗИ и СФ;

- общие сведения о защищаемой информации, используемой в процессе эксплуатации СКЗИ;

- сведения о каналах связи, по которым передаются защищаемые СКЗИ персональные данные (далее - канал связи);

- все возможные данные, передаваемые в открытом виде по каналам связи, не защищенным от несанкционированного доступа к информации организационными и техническими мерами;

- сведения обо всех проявляющихся в каналах связи, не защищенных от несанкционированного доступа к информации организационными и техническими мерами, нарушениях правил эксплуатации СКЗИ и СФ;

- сведения обо всех проявляющихся в каналах связи, не защищенных от несанкционированного доступа к информации организационными и техническими мерами, неисправностях и сбоях аппаратных компонентов СКЗИ и СФ;

- сведения, получаемые в результате анализа любых сигналов от аппаратных компонентов СКЗИ и СФ;

ж) применение:

- находящихся в свободном доступе или используемых за пределами контролируемой зоны АС и ПО, включая аппаратные и программные компоненты СКЗИ и СФ;

- специально разработанных АС и ПО;

з) использование на этапе эксплуатации в качестве среды переноса от субъекта к объекту (от объекта к субъекту) атаки действий, осуществляемых при подготовке и (или) проведении атаки:

- каналов связи, не защищенных от несанкционированного доступа к информации организационными и техническими мерами;

- каналов распространения сигналов, сопровождающих функционирование СКЗИ и СФ;

и) проведение на этапе эксплуатации атаки из

www.alfario.ru

информационно-телекоммуникационных сетей, доступ к которым не ограничен определенным кругом лиц, если информационные системы, в которых используются СКЗИ, имеют выход в эти сети;

к) использование на этапе эксплуатации находящихся за пределами контролируемой зоны АС и ПО из состава средств информационной системы, применяемых на местах эксплуатации СКЗИ (далее - штатные средства).

11. СКЗИ **класса КС2** применяются для нейтрализации атак, при создании способов, подготовке и проведении которых используются возможности из числа перечисленных в **пункте 10** настоящего документа и не менее одной из следующих дополнительных возможностей:

а) проведение атаки при нахождении в пределах контролируемой зоны;

б) проведение атак на этапе эксплуатации СКЗИ на следующие объекты:

- документацию на СКЗИ и компоненты СФ;

- помещения, в которых находится совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем (далее - СВТ), на которых реализованы СКЗИ и СФ;

в) получение в рамках предоставленных полномочий, а также в результате наблюдений следующей информации:

- сведений о физических мерах защиты объектов, в которых размещены ресурсы информационной системы;

- сведений о мерах по обеспечению контролируемой зоны объектов, в которых размещены ресурсы информационной системы;

- сведений о мерах по разграничению доступа в Помещения, в которых находятся СВТ, на которых реализованы СКЗИ и СФ;

г) использование штатных средств, ограниченное мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий.

12. СКЗИ **класса КС3** применяются для нейтрализации атак, при создании способов, подготовке и проведении которых используются возможности из числа перечисленных в **пунктах 10** и **11** настоящего документа и не менее одной из следующих дополнительных возможностей:

а) физический доступ к СВТ, на которых реализованы СКЗИ и СФ;

б) возможность располагать аппаратными компонентами СКЗИ и СФ, ограниченная мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий.

13. СКЗИ **класса КВ** применяются для нейтрализации атак, при создании способов, подготовке и проведении которых используются возможности из числа перечисленных в **пунктах 10 - 12** настоящего документа и не менее одной из следующих дополнительных возможностей:

а) создание способов, подготовка и проведение атак с привлечением специалистов в области анализа сигналов, сопровождающих функционирование СКЗИ и СФ, и в области использования для реализации атак недокументированных (не декларированных) возможностей прикладного ПО;

б) проведение лабораторных исследований СКЗИ, используемых вне контролируемой зоны, ограниченное мерами, реализованными в информационной

www.alfario.ru

системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий;

в) проведение работ по созданию способов и средств атак в научно-исследовательских центрах, специализирующихся в области разработки и анализа СКЗИ и СФ, в том числе с использованием исходных текстов входящего в СФ прикладного ПО, непосредственно использующего вызовы программных функций СКЗИ.

14. СКЗИ класса КА применяются для нейтрализации атак, при создании способов, подготовке и проведении которых используются возможности из числа перечисленные в **пунктах 10 - 13** настоящего документа и не менее одной из следующих дополнительных возможностей:

а) создание способов, подготовка и проведение атак с привлечением специалистов в области использования для реализации атак недокументированных (не декларированных) возможностей системного ПО;

б) возможность располагать сведениями, содержащимися в конструкторской документации на аппаратные и программные компоненты СФ;

в) возможность располагать всеми аппаратными компонентами СКЗИ и СФ.

15. В процессе формирования совокупности предположений о возможностях, которые могут использоваться при создании способов, подготовке и проведении атак, дополнительные возможности, не входящие в число перечисленных в **пунктах 10 - 14** настоящего документа, не влияют на порядок определения требуемого класса СКЗИ.

III. Состав и содержание организационных и технических мер, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для 3 уровня защищенности

16. В соответствии с **пунктом 14** Требований к защите персональных данных для обеспечения 3 уровня защищенности персональных данных при их обработке в информационных системах помимо выполнения требований, предусмотренных **пунктом 5** настоящего документа, необходимо выполнение требования о назначении должностного лица (работника), ответственного за обеспечение безопасности персональных данных в информационной системе.

17. Для выполнения требования, указанного в **пункте 16** настоящего документа, необходимо назначение обладающего достаточными навыками должностного лица (работника) оператора ответственным за обеспечение безопасности персональных данных в информационной системе.

18. Для выполнения требования, указанного в **подпункте «г» пункта 5** настоящего документа, необходимо вместо меры, предусмотренной **подпунктом «в» пункта 9** настоящего документа, использовать для обеспечения требуемого уровня защищенности персональных данных при их обработке в информационной системе:

- СКЗИ **класса КВ** и выше в случаях, когда для информационной системы актуальны **угрозы 2 типа**;

- СКЗИ **класса КС1** и выше в случаях, когда для информационной системы актуальны **угрозы 3 типа**.

www.alfario.ru

IV. Состав и содержание организационных и технических мер, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для 2 уровня защищенности

19. В соответствии с **пунктом 15** Требований к защите персональных данных для обеспечения 2 уровня защищенности персональных данных при их обработке в информационных системах помимо выполнения требований, предусмотренных **пунктами 5** и **16** настоящего документа, необходимо выполнение требования о том, чтобы доступ к содержанию электронного журнала сообщений был возможен исключительно для должностных лиц (работников) оператора или уполномоченного лица, которым сведения, содержащиеся в указанном журнале, необходимы для выполнения служебных (трудовых) обязанностей.

20. Для выполнения требования, указанного в **пункте 19** настоящего документа, необходимо:

а) утверждение руководителем оператора списка лиц, допущенных к содержанию электронного журнала сообщений, и поддержание указанного списка в актуальном состоянии;

б) обеспечение информационной системы автоматизированными средствами, регистрирующими запросы пользователей информационной системы на получение персональных данных, а также факты предоставления персональных данных по этим запросам в электронном журнале сообщений;

в) обеспечение информационной системы автоматизированными средствами, исключающими доступ к содержанию электронного журнала сообщений лиц, не указанных в утвержденном руководителем оператора списке лиц, допущенных к содержанию электронного журнала сообщений;

г) обеспечение периодического контроля работоспособности указанных в **подпунктах «б»** и **«в»** настоящего пункта автоматизированных средств (не реже 1 раза в полгода).

21. Для выполнения требования, указанного в **подпункте «г» пункта 5** настоящего документа, необходимо вместо мер, предусмотренных **подпунктом «в» пункта 9** и **пунктом 18** настоящего документа, использовать для обеспечения требуемого уровня защищенности персональных данных при их обработке в информационной системе:

- СКЗИ **класса КА** в случаях, когда для информационной системы актуальны **угрозы 1 типа**;
- СКЗИ **класса КВ** и выше в случаях, когда для информационной системы актуальны **угрозы 2 типа**;
- СКЗИ **класса КС1** и выше в случаях, когда для информационной системы актуальны **угрозы 3 типа**.

V. Состав и содержание организационных и технических мер, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для 1 уровня защищенности

22. В соответствии с **пунктом 16** Требований к защите персональных данных для обеспечения **1 уровня защищенности** персональных данных при их обработке в

www.alfario.ru

информационных системах помимо выполнения требований, предусмотренных **пунктами 5**, **16** и **19** настоящего документа, необходимо выполнение следующих требований:

а) автоматическая регистрация в электронном журнале безопасности изменения полномочий сотрудника оператора по доступу к персональным данным, содержащимся в информационной системе;

б) создание отдельного структурного подразделения, ответственного за обеспечение безопасности персональных данных в информационной системе, либо возложение его функций на одно из существующих структурных подразделений.

23. Для выполнения требования, указанного в **подпункте «а» пункта 22** настоящего документа, необходимо:

а) обеспечение информационной системы автоматизированными средствами, позволяющими автоматически регистрировать в электронном журнале безопасности изменения полномочий сотрудника оператора по доступу к персональным данным, содержащимся в информационной системе;

б) отражение в электронном журнале безопасности полномочий сотрудников оператора персональных данных по доступу к персональным данным, содержащимся в информационной системе. Указанные полномочия должны соответствовать должностным обязанностям сотрудников оператора;

в) назначение оператором лица, ответственного за периодический контроль ведения электронного журнала безопасности и соответствия, отраженных в нем полномочий сотрудников оператора их должностным обязанностям (не реже 1 раза в месяц).

24. Для выполнения требования, указанного в **подпункте «б» пункта 22** настоящего документа, необходимо:

а) провести анализ целесообразности создания отдельного структурного подразделения, ответственного за обеспечение безопасности персональных данных в информационной системе;

б) создать отдельное структурное подразделение, ответственное за обеспечение безопасности персональных данных в информационной системе, либо возложить его функции на одно из существующих структурных подразделений.

25. Для выполнения требования, указанного в **подпункте «а» пункта 5** настоящего документа, для обеспечения **1 уровня защищенности** необходимо:

а) оборудовать окна Помещений, расположенные на первых и (или) последних этажах зданий, а также окна Помещений, находящиеся около пожарных лестниц и других мест, откуда возможно проникновение в Помещения посторонних лиц, металлическими решетками или ставнями, охранной сигнализацией или другими средствами, препятствующими неконтролируемому проникновению посторонних лиц в помещения;

б) оборудовать окна и двери Помещений, в которых размещены серверы информационной системы, металлическими решетками, охранной сигнализацией или другими средствами, препятствующими неконтролируемому проникновению посторонних лиц в помещения.

26. Для выполнения требования, указанного в **подпункте «г» пункта 5** настоящего документа, необходимо вместо мер, предусмотренных **подпунктом «в» пункта 9**, **пунктами 18** и **21** настоящего документа, использовать для обеспечения

www.alfario.ru

требуемого уровня защищенности персональных данных при их обработке в информационной системе:

- СКЗИ **класса КА** в случаях, когда для информационной системы актуальны **угрозы 1 типа**;

- СКЗИ **класса КВ** и выше в случаях, когда для информационной системы актуальны **угрозы 2 типа**.

---

* Собрание законодательства Российской Федерации, 2012, № 45, 6257.

** К этапам жизненного цикла СКЗИ относятся разработка (модернизация) указанных средств, их производство, хранение, транспортировка, ввод в эксплуатацию (пусконаладочные работы), эксплуатация.

*** Границей контролируемой зоны могут быть периметр охраняемой территории предприятия (учреждения), ограждающие конструкции охраняемого здания, охраняемой части здания, выделенного помещения.

www.alfario.ru