УТВЕРЖДЕНЫ
приказом ФСТЭК России
от « 30 » июля 2018 г. № 132

Зарегистрирован Минюстом России
« 14 » ноября 2018 г. № 52687

Требования по безопасности информации к средствам защиты информации от воздействий, направленных на отказ в обслуживании информационных (автоматизированных) систем
(выписка)

I. Общие положения

1. Настоящие Требования являются обязательными требованиями в области технического регулирования к продукции (работам, услугам), используемой в целях защиты сведений, составляющих государственную тайну или относимых к охраняемой в соответствии с законодательством Российской Федерации иной информации ограниченного доступа (далее – требования по безопасности информации), применяются к программным и программно-техническим средствам защиты информации, содержащей сведения, составляющие государственную тайну, иной информации ограниченного доступа, реализующим функции защиты от воздействий, направленных на отказ в обслуживании информационных (автоматизированных) систем, подключенных к сетям связи (далее – средства защиты от воздействий типа «отказ в обслуживании»).

Настоящие Требования не распространяются на средства государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации.

2. Настоящие Требования разработаны в соответствии с постановлением Правительства Российской Федерации от 26 июня 1995 г. № 608 «О сертификации средств защиты информации» (Собрание законодательства Российской Федерации, 1995, № 27, ст. 2579; 1996, № 18, ст. 2142; 1999, № 14, ст. 1722; 2004, № 52, ст. 5480; 2010, № 18, ст. 2238), постановлением Правительства Российской Федерации от 15 мая 2010 г. № 330 «Об особенностях оценки соответствия продукции (работ, услуг), используемой в целях защиты сведений, относимых к охраняемой в соответствии с законодательством Российской Федерации информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну, а также процессов ее проектирования (включая изыскания), производства, строительства, монтажа, наладки, эксплуатации,

хранения, перевозки, реализации, утилизации и захоронения», приказом ФСТЭК России от 3 апреля 2018 г. № 55 «Об утверждении Положения о системе сертификации средств защиты информации» (зарегистрирован Минюстом России 11 мая 2018 г., регистрационный № 51063; официальный интернет-портал правовой информации http://www.pravo.gov.ru, 14 мая 2018 г.).

3. Настоящие Требования включают общие требования к средствам защиты от воздействий типа «отказ в обслуживании» и минимально необходимые требования к функциям безопасности средств защиты от воздействий типа «отказ в обслуживании».

При включении в средство защиты от воздействий типа «отказ в обслуживании» дополнительных функций безопасности требования к таким функциям безопасности должны быть заданы в технических условиях или задании по безопасности и оценены при проведении сертификации средства защиты от воздействий типа «отказ в обслуживании».

4. Выполнение настоящих Требований является обязательным при проведении работ по оценке соответствия (включая работы по сертификации) средств технической защиты информации и средств обеспечения безопасности информационных технологий, организуемых ФСТЭК России в пределах своих полномочий в соответствии с Положением о системе сертификации средств защиты информации, утвержденным приказом ФСТЭК России от 3 апреля 2018 г. № 55.

II. Общие требования к средствам защиты от воздействий типа «отказ в обслуживании»

5. Средства защиты от воздействий типа «отказ в обслуживании» являются элементом систем защиты информации информационных (автоматизированных) систем и применяются вместе с другими средствами защиты информации.

6. Средства защиты от воздействий типа «отказ в обслуживании» должны обеспечивать защиту информационных (автоматизированных) систем от всех возможных типов воздействий, направленных на отказ в обслуживании информационных (автоматизированных) систем, в том числе от воздействий, связанных с переполнением полосы пропускания, недостатком вычислительных ресурсов, ошибками программирования, а также от воздействий на сервера доменных имен (DNS-сервера).

Средства защиты от воздействий типа «отказ в обслуживании» должны обнаруживать попытки осуществления воздействий, направленных на отказ в обслуживании информационных (автоматизированных) систем, на основе анализа сетевого трафика.

7. В средства защиты от воздействий типа «отказ в обслуживании» должны входить компоненты анализа сетевого трафика (датчики или сенсоры), компоненты

обработки сетевого трафика, содержащего сетевые пакеты, используемые нарушителем для осуществления воздействий, направленных на отказ в обслуживании информационных (автоматизированных) систем (анализаторы и очистители), компоненты базы решающих правил, а также средства организации взаимодействия.

8. В средствах защиты от воздействий типа «отказ в обслуживании» обнаружение попыток осуществления воздействий, направленных на отказ в обслуживании информационных (автоматизированных) систем, должно реализовываться следующими методами:

сигнатурными методами, основанными на признаках (сигнатурах) сетевого трафика;

статистическими методами, основанными на профилях функционирования информационной (автоматизированной) системы.

В средствах защиты от воздействий типа «отказ в обслуживании» могут быть реализованы дополнительные методы обнаружения в общем объеме сетевого трафика сетевых пакетов, используемых нарушителем для осуществления воздействий, направленных на отказ в обслуживании информационных (автоматизированных) систем, и их обработки.

9. Для дифференциации требований по безопасности информации к средствам защиты от воздействий типа «отказ в обслуживании» выделяются четыре класса защиты средств защиты от воздействий типа «отказ в обслуживании». Самый низкий класс – шестой, самый высокий – третий.

Средства защиты от воздействий типа «отказ в обслуживании», соответствующие 6 классу защиты, применяются на значимых объектах критической информационной инфраструктуры 3 категории[1], в государственных информационных системах 3 класса защищенности[**], в автоматизированных системах управления производственными и технологическими процессами 3 класса защищенности[***], в информационных системах персональных данных при

1[*] Устанавливается в соответствии со статьей 7 Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» (Собрание законодательства Российской Федерации, 2017, № 31, ст. 4736) и Правилами категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечнем показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации, утвержденными постановлением Правительства Российской Федерации от 8 февраля 2018 г. № 127 (Собрание законодательства Российской Федерации, 2018, № 8, ст. 1204).

2[**] Устанавливается в соответствии с Требованиями о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденными приказом ФСТЭК России от 11 февраля 2013 г. № 17 (зарегистрирован Минюстом России 31 мая 2013 г., регистрационный № 28608) (с изменениями, внесенными приказом ФСТЭК России от 15 февраля 2017 г. № 27 (зарегистрирован Минюстом России 14 марта 2017 г., регистрационный № 45933; Официальный интернет-портал правовой информации http://www.pravo.gov.ru, 15 марта 2017 г.).

3[*] Устанавливается в соответствии со статьей 7 Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» (Собрание законодательства Российской Федерации, 2017, № 31, ст. 4736) и Правилами категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечнем показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации, утвержденными постановлением Правительства Российской Федерации от 8 февраля 2018 г. № 127 (Собрание законодательства Российской Федерации, 2018, № 8, ст. 1204).

необходимости обеспечения 3 и 4 уровней защищенности персональных данных[****].

Средства защиты от воздействий типа «отказ в обслуживании», соответствующие 5 классу защиты, применяются на значимых объектах критической информационной инфраструктуры 2 категории[*], в государственных информационных системах 2 класса защищенности[**], в автоматизированных системах управления производственными и технологическими процессами 2 класса защищенности[***], в информационных системах персональных данных при необходимости обеспечения 2 уровня защищенности персональных данных[****].

Средства защиты от воздействий типа «отказ в обслуживании», соответствующие 4 классу защиты, применяются на значимых объектах критической информационной инфраструктуры 1 категории[*], в государственных информационных системах 1 класса защищенности[**], в автоматизированных системах управления производственными и технологическими процессами 1 класса защищенности[***], в информационных системах персональных данных при необходимости обеспечения 1 уровня защищенности персональных данных[****], в информационных системах общего пользования II класса[*****].

10. Средства защиты от воздействий типа «отказ в обслуживании» должны соответствовать требованиям по безопасности информации, устанавливающим уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий, утверждаемым ФСТЭК России в соответствии с подпунктом 13.1 пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утвержденного Указом Президента Российской Федерации от 16 августа 2004 г. № 1085.

Средства защиты от воздействий типа «отказ в обслуживании» 6 класса защиты должны соответствовать требованиям к 6 уровню доверия.

Средства защиты от воздействий типа «отказ в обслуживании» 5 класса защиты должны соответствовать требованиям к 5 уровню доверия.

[**] Устанавливается в соответствии с Требованиями о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденными приказом ФСТЭК России от 11 февраля 2013 г. № 17 (зарегистрирован Минюстом России 31 мая 2013 г., регистрационный № 28608) (с изменениями, внесенными приказом ФСТЭК России от 15 февраля 2017 г. № 27 (зарегистрирован Минюстом России 14 марта 2017 г., регистрационный № 45933; Официальный интернет-портал правовой информации http://www.pravo.gov.ru, 15 марта 2017 г.).

[***] Устанавливается в соответствии с Требованиями к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды, утвержденными приказом ФСТЭК России от 14 марта 2014 г. № 31 (зарегистрирован Минюстом России 30 июня 2014 г., регистрационный № 32919) (с изменениями, внесенными приказом ФСТЭК России от 23 марта 2017 г. № 49 (зарегистрирован Минюстом России 30 июня 2017 г., регистрационный № 32919; Официальный интернет-портал правовой информации http://www.pravo.gov.ru, 26 апреля 2017 г.) и приказом ФСТЭК России от 9 августа 2018 г. № 138 (зарегистрирован Минюстом России 5 сентября 2018 г., регистрационный № 52071; Официальный интернет-портал правовой информации http://www.pravo.gov.ru, 6 сентября 2018 г.).

4[****] Устанавливается в соответствии с Требованиями к защите персональных данных при их обработке в информационных системах персональных данных, утвержденными постановлением Правительства Российской Федерации от 1 ноября 2012 г., № 1119 (Собрание законодательства Российской Федерации, 2012, № 45, ст. 6257).

5[*****] Устанавливается в соответствии с Требованиями о защите информации, содержащейся в информационных системах общего пользования, утвержденными приказом ФСБ России и ФСТЭК России от 31 августа 2010 г. № 416/489 (зарегистрирован Минюстом России 13 октября 2010 г., регистрационный № 18704).

Средства защиты от воздействий типа «отказ в обслуживании» 4 класса защиты должны соответствовать требованиям к 4 уровню доверия.

11. В среде функционирования средств защиты от воздействий типа «отказ в обслуживании» должна обеспечиваться защита их компонентов от несанкционированного доступа в соответствии с требованиями, предъявляемыми к информационной (автоматизированной) системе, в которой функционирует средство защиты от воздействий типа «отказ в обслуживании».

Для средств защиты от воздействий типа «отказ в обслуживании» должны быть обеспечены количественные характеристики сетевого трафика (объем, скорость), предназначенного для обработки этими средствами, не превышающие значений, установленных эксплуатационной документацией на средства защиты от воздействий типа «отказ в обслуживании».

III. Требования к функциям безопасности средств защиты от воздействий типа «отказ в обслуживании»

12. Средство защиты от воздействий типа «отказ в обслуживании» удовлетворяет требованиям к функциям безопасности, если в нем реализованы функции безопасности, приведенные в таблице 1.

Таблица 1

№ п/п	Наименование функции безопасности	Класс защиты		
		6	5	4
1.	Анализ сетевого трафика	+	+	+
2.	Регистрация событий безопасности, связанных с попытками осуществления воздействий, направленных на отказ в обслуживании информационных (автоматизированных) систем	+	=	+
3.	Реагирование на события безопасности, связанные с попытками осуществления воздействий, направленных на отказ в обслуживании информационных (автоматизированных) систем	+	+	+
4.	Поддержка базы решающих правил средства защиты от воздействий типа «отказ в обслуживании»	+	=	=
5.	Создание профилей функционирования информационной (автоматизированной) системы	+	+	+
6.	Управление (администрирование) средством защиты от воздействий типа «отказ в обслуживании»	+	=	=
7.	Регистрация событий безопасности, связанных с функционированием средства защиты от воздействий типа «отказ в обслуживании»	+	+	+
8.	Обеспечение доверенного канала для взаимодействия между компонентами средства защиты от воздействий типа «отказ в обслуживании»	+	=	=
9.	Обеспечение целостности средства защиты от воздействий типа «отказ в обслуживании»	+	=	=

Обозначение «+» в строке функции безопасности указывает на наличие требований, предъявляемых к данной функции безопасности, для соответствующего класса защиты средств защиты от воздействий типа «отказ в обслуживании».

Обозначение «=» означает, что требования соответствуют требованиям, предъявляемым к предыдущему классу защиты средств защиты от воздействий типа «отказ в обслуживании».

Требования к функциям безопасности средства защиты от воздействий типа «отказ в обслуживании» 6 класса защиты

13. Для реализации функции безопасности по анализу сетевого трафика средство защиты от воздействий типа «отказ в обслуживании» должно:

1) содержать механизм анализа сетевого трафика с целью обнаружения попыток осуществления воздействий, направленных на отказ в обслуживании информационной (автоматизированной) системы;

2) анализировать сетевой трафик с использованием следующих методов анализа:

сигнатурных методов, основанных на признаках (сигнатурах) сетевого трафика;

статистических методов, основанных на профилях функционирования информационной (автоматизированной) системы (определение «нормального» и «аномального» сетевого трафика);

3) анализировать следующие атрибуты сетевого трафика:

заголовки сетевых пакетов;

используемые сетевые адреса источника сетевого трафика и получателя;

используемые сетевые протоколы;

количество и объем передаваемой информации в единицу времени;

4) содержать механизм выявления попыток осуществления воздействий, направленных на отказ в обслуживании информационной (автоматизированной) системы, на основании профилей функционирования информационной (автоматизированной) системы;

5) использовать для выявления попыток осуществления воздействий, направленных на отказ в обслуживании информационной (автоматизированной) системы, профили функционирования информационной (автоматизированной) системы.

14. Для реализации функции безопасности по регистрации событий безопасности, связанных с попытками осуществления воздействий, направленных на отказ в обслуживании информационной (автоматизированной) системы в каждой записи аудита средством защиты от воздействий типа «отказ в обслуживании» должна регистрироваться следующая информация:

дата и время попытки реализации воздействия;

продолжительность попытки реализации воздействия;

объект, на который была направлена попытка реализации воздействия;

скорость и объем аномального трафика.

15. Для реализации функции безопасности по реагированию на события безопасности, связанные с попытками осуществления воздействий, направленных на отказ в обслуживании информационных (автоматизированных) систем, средство защиты от воздействий типа «отказ в обслуживании» должно:

содержать механизм уведомления (оповещения) администратора об обнаружении событий безопасности, связанных с отказом в обслуживании;

обеспечивать возможность передачи управляющего сигнала в средства межсетевого экранирования (и/или иное телекоммуникационное оборудование, и/или иные средства защиты информации) для применения правил фильтрации сетевых пакетов.

16. Для реализации функции безопасности по поддержке базы решающих правил средства защиты от воздействий типа «отказ в обслуживании» в средстве защиты от воздействий типа «отказ в обслуживании» должна быть предусмотрена база решающих правил.

Предустановленные решающие правила должны обеспечивать корректность обнаружения и классификации воздействий типа «отказ в обслуживании».

Средство защиты от воздействий типа «отказ в обслуживании» должно содержать:

механизм создания решающих правил;

механизм включения и отключения решающих правил;

механизм обновления базы решающих правил, предоставляемой заявителем на сертификацию в соответствии с регламентом обновления базы решающих правил.

17. Для реализации функции безопасности по созданию профилей функционирования информационной (автоматизированной) системы средство защиты от воздействий типа «отказ в обслуживании» должно:

предусматривать режим обучения, в котором осуществляется регистрация основных атрибутов сетевых пакетов с целью построения контрольных характеристик сетевого трафика;

содержать механизм создания профилей функционирования информационной (автоматизированной) системы на основе контрольных характеристик сетевого трафика;

обеспечивать возможность создания:

профилей нормального функционирования информационной (автоматизированной) системы;

профилей функционирования информационной (автоматизированной) системы

на основе собранных данных о сетевом трафике информационной (автоматизированной) системы.

В средстве защиты от воздействий типа «отказ в обслуживании» должен быть реализован механизм сохранения профилей функционирования информационной (автоматизированной) системы.

18. Для реализации функции безопасности по управлению (администрированию) средством защиты от воздействий типа «отказ в обслуживании» в средстве должен быть реализован графический интерфейс управления средством защиты от воздействий типа «отказ в обслуживании» со стороны администраторов.

Средство защиты от воздействий типа «отказ в обслуживании» должно обеспечивать:

идентификацию и аутентификацию администраторов средства защиты от воздействий типа «отказ в обслуживании»;

возможность управления доступом к функциональным возможностям управления (администрирования) средства защиты от воздействий типа «отказ в обслуживании» на основе ролей;

возможность управления параметрами настройки средства защиты от воздействий типа «отказ в обслуживании», определяющими режимы выполнения функций безопасности;

возможность управления данными, собранными или созданными средством защиты от воздействий типа «отказ в обслуживании», со стороны администраторов;

возможность настройки сроков хранения информации о зарегистрированных событиях безопасности.

Средством защиты от воздействий типа «отказ в обслуживании» или средой его должен обеспечиваться доверенный канал для администрирования средства защиты от воздействий типа «отказ в обслуживании».

При осуществлении удаленного администрирования по каналам связи, имеющим выходы за пределы установленной в организации контролируемой зоны, доверенный канал должен обеспечиваться за счет применения сертифицированных средств криптографической защиты информации.

19. Для реализации функции безопасности по регистрации событий безопасности, связанных с функционированием средства защиты от воздействий типа «отказ в обслуживании», средство должно:

содержать механизм регистрации событий безопасности, связанных с функционированием средства защиты от воздействий типа «отказ в обслуживании»;

обеспечивать возможность регистрации:

доступа к функциональным возможностям управления (администрирования) средства защиты от воздействий типа «отказ в обслуживании»;

событий, связанных с действиями по управлению данными, собранными или

созданными средством защиты от воздействий типа «отказ в обслуживании».

20. Для реализации функции безопасности по обеспечению доверенного канала для взаимодействия между компонентами средства защиты от воздействий типа «отказ в обслуживании» средством защиты или средой его функционирования должен обеспечиваться доверенный канал для взаимодействия между компонентами средства защиты от воздействий типа «отказ в обслуживании».

При осуществлении взаимодействия между компонентами средства защиты от воздействий типа «отказ в обслуживании» по каналам связи, имеющим выходы за пределы установленной в организации контролируемой зоны, доверенный канал должен обеспечиваться за счет применения сертифицированных средств криптографической защиты информации.

21. Для реализации функции безопасности по обеспечению целостности средства защиты от воздействий типа «отказ в обслуживании» средство должно обеспечивать целостность программного обеспечения, обновлений базы решающих правил и параметров настройки средства защиты от воздействий типа «отказ в обслуживании», а также хранимых средством данных путем применения криптографических механизмов обеспечения и контроля целостности.

Требования к функциям безопасности средства защиты от воздействий типа «отказ в обслуживании» 5 класса защиты

22. Для реализации функции безопасности по анализу сетевого трафика наряду с требованиями, установленными пунктом 13 настоящих Требований, средство защиты от воздействий типа «отказ в обслуживании» должно анализировать информацию об атрибутах сетевого трафика, передаваемого к узлам информационной (автоматизированной) системы:

флаги (биты) управления сетевым соединением, передачей и получением информации;

заголовки протоколов прикладного уровня.

23. Требования по регистрации событий безопасности, связанных с попытками осуществления воздействий, направленных на отказ в обслуживании информационных (автоматизированных) систем, совпадают с требованиями, установленными пунктом 14 настоящих Требований.

24. Для реализации функции безопасности по реагированию на события безопасности, связанные с попытками осуществления воздействий, направленных на отказ в обслуживании информационных (автоматизированных) систем, наряду с требованиями, установленными пунктом 15 настоящих Требований, средство защиты от воздействий типа «отказ в обслуживании» должно реализовывать:

выполнение очистки сетевого трафика от нелегитимных сетевых пакетов (определяются на основе решающих правил, профилей функционирования

информационной (автоматизированной) системы и информации об атрибутах сетевого трафика);

уменьшение скорости и (или) объема передаваемой информации к узлу информационной (автоматизированной) системы (с учетом суммарных количественных характеристик сетевого трафика и (или) его направления);

фильтрацию сетевого трафика в соответствии с заданными и (или) динамически формируемыми правилами.

25. Требования по поддержке базы решающих правил средства защиты от воздействий типа «отказ в обслуживании» соответствуют требованиям, установленным пунктом 16 настоящих Требований.

26. Для реализации функции безопасности по созданию профилей функционирования информационной (автоматизированной) системы наряду с требованиями, установленными пунктом 17 настоящих Требований, средство защиты от воздействий типа «отказ в обслуживании» должно обеспечивать возможность создания профилей функционирования информационной (автоматизированной) системы на основе собранных данных об обращениях к ресурсам информационной (автоматизированной) системы.

27. Требования по управлению (администрированию) средством защиты от воздействий типа «отказ в обслуживании» соответствуют требованиям, установленным пунктом 18 настоящих Требований.

28. Для реализации функции безопасности по регистрации событий безопасности, связанных с функционированием средства защиты от воздействий типа «отказ в обслуживании», наряду с требованиями, установленными пунктом 19 настоящих Требований, средство защиты от воздействий типа «отказ в обслуживании» должно обеспечивать возможность регистрации событий, связанных с действиями по управлению параметрами настройки средства защиты от воздействий типа «отказ в обслуживании», определяющими режимы выполнения функций безопасности.

29. Требования по обеспечению доверенного канала для взаимодействия между компонентами средства защиты от воздействий типа «отказ в обслуживании» соответствуют требованиям, установленным пунктом 20 настоящих Требований.

30. Требования по обеспечению целостности средства защиты от воздействий типа «отказ в обслуживании» совпадают с требованиями, установленными пунктом 21 настоящих Требований.

Требования к функциям безопасности средства защиты от воздействий типа «отказ в обслуживании» 4 класса защиты

31. Для реализации функции безопасности по анализу сетевого трафика наряду с требованиями, установленными пунктом 22 настоящих Требований, средство

защиты от воздействий типа «отказ в обслуживании» должно анализировать информацию об интерфейсах телекоммуникационного оборудования, участвующего в получении и передаче сетевого трафика, а также типах сервисов, используемых для определения приоритетов обработки сетевого трафика.

32. Для реализации функции безопасности по регистрации событий безопасности, связанных с попытками осуществления воздействий, направленных на отказ в обслуживании информационных (автоматизированных) систем, наряду с требованиями, установленными пунктом 14 настоящих Требований, каждая запись аудита дополнительно должна включать информацию о результатах реагирования на события безопасности, связанные с попытками осуществления воздействий, направленных на отказ в обслуживании.

33. Для реализации функции безопасности по реагированию на события безопасности, связанные с попытками осуществления воздействий, направленных на отказ в обслуживании информационных (автоматизированных) систем, наряду с требованиями, установленными пунктом 24 настоящих Требований, средство защиты от воздействий типа «отказ в обслуживании» дополнительно должно реализовывать:

отправку управляющего сигнала на средства межсетевого экранирования (и/или иное телекоммуникационное оборудование, и/или иные средства защиты информации) для перенаправления сетевого трафика в его логический интерфейс, не предназначенный для обработки сетевого трафика;

разрыв неактивных сетевых сессий.

34. Требования по поддержке базы решающих правил средства защиты от воздействий типа «отказ в обслуживании» соответствуют требованиям, установленным пунктом 16 настоящих Требований.

35. Для реализации функции безопасности по созданию профилей функционирования информационной (автоматизированной) системы наряду с требованиями, установленными пунктом 26 настоящих Требований, средство защиты от воздействий типа «отказ в обслуживании» дополнительно должно обеспечивать возможность создания:

профилей аномалий функционирования информационной (автоматизированной) системы;

профилей функционирования информационной (автоматизированной) системы на основе собранных данных о штатном и аномальном функционировании информационной (автоматизированной) системы с использованием мониторинга режимов функционирования сетевого оборудования, в том числе сетевых компонентов средств защиты информации (на основе информации об активном соединении, содержащейся в стандартных сетевых протоколах).

36. Требования по управлению (администрированию) средством защиты от воздействий типа «отказ в обслуживании» соответствуют требованиям, установленным пунктом 18 настоящих Требований.

37. Для реализации функции безопасности по регистрации событий безопасности, связанных с функционированием средства защиты от воздействий типа «отказ в обслуживании», наряду с требованиями, установленными пунктом 28 настоящих Требований, средство защиты от воздействий типа «отказ в обслуживании» дополнительно должно обеспечивать возможность отображения сведений о направлениях (векторах) воздействий, направленных на отказ в обслуживании.

38. Требования по обеспечению доверенного канала для взаимодействия между компонентами средства защиты от воздействий типа «отказ в обслуживании» совпадают с требованиями, установленными пунктом 20 настоящих Требований.

39. Требования по обеспечению целостности средства защиты от воздействий типа «отказ в обслуживании» соответствуют требованиям, установленным пунктом 21 настоящих Требований.