УТВЕРЖДЕНЫ
приказом ФСТЭК России
от « 7 » марта 2023 г. № 44

Требования по безопасности информации к многофункциональным межсетевым экранам уровня сети (выписка)

1. Настоящие Требования являются обязательными в области технического регулирования к продукции, используемой в целях защиты сведений, составляющих государственную тайну или относимых к охраняемой в соответствии с законодательством Российской Федерации иной информации ограниченного доступа[1] (далее – требования по безопасности информации), предъявляемыми к программно-аппаратным средствам, реализующим фильтрацию, контроль доступа в информационную (автоматизированную) систему, контроль за информацией, поступающей в информационную (автоматизированную) систему и (или) выходящей из информационной (автоматизированной) системы, и обеспечивающим защиту информационной (автоматизированной) системы от угроз безопасности информации, связанных с подключением к сетям связи общего пользования (далее – многофункциональные межсетевые экраны уровня сети).

2. 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 (зарегистрирован Минюстом России 11 мая 2018 г., регистрационный № 51063) (с изменениями, внесенными приказами ФСТЭК России от 5 августа 2021 г. № 121 (зарегистрирован Минюстом России 27 октября 2021 г., регистрационный № 65594) и от 19 сентября 2022 г. № 172 (зарегистрирован Минюстом России 19 октября 2022 г., регистрационный № 70614).

3. К многофункциональным межсетевым экранам уровня сети устанавливается 3 класса защиты.

Многофункциональные межсетевые экраны уровня сети,

[1] Статья 5 Федерального закона от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании».

соответствующие 6 классу защиты, применяются в значимых объектах критической информационной инфраструктуры 3 категории значимости[2], в государственных информационных системах 3 класса защищенности[3], в автоматизированных системах управления производственными и технологическими процессами 3 класса защищенности[4], в информационных системах персональных данных при необходимости обеспечения 3 и 4 уровня защищенности персональных данных[5].

Многофункциональные межсетевые экраны уровня сети, соответствующие 5 классу защиты, применяются в значимых объектах критической информационной инфраструктуры 2 категории значимости, 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.

Многофункциональные межсетевые экраны уровня сети, соответствующие 4 классу защиты, применяются в значимых объектах критической информационной инфраструктуры 1 категории значимости, 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[6].

5. Требования по безопасности информации предъявляются к:

уровню доверия многофункционального межсетевого экрана уровня сети;

управлению доступом в многофункциональном межсетевом экране уровня

---

[2] Статья 7 Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», Правила категорирования объектов критической информационной инфраструктуры Российской Федерации, утвержденные постановлением Правительства Российской Федерации от 8 февраля 2018 г. № 127.

[3] Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденные 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) и приказом ФСТЭК России от 28 мая 2019 г. № 106 (зарегистрирован Минюстом России 13 сентября 2019 г., регистрационный № 55924).

[4] Требования 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, утвержденные 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 25 апреля 2017 г., регистрационный № 46487), приказом ФСТЭК России от 9 августа 2018 г. № 138 (зарегистрирован Минюстом России 5 сентября 2018 г., регистрационный № 52071) и приказом ФСТЭК России от 15 марта 2021 г. № 46 (зарегистрирован Минюстом России 1 июля 2021 г., регистрационный № 64063).

[5] Требования к защите персональных данных при их обработке в информационных системах персональных данных, утвержденные постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119.

[6] Требования о защите информации, содержащейся в информационных системах общего пользования, утвержденные приказом ФСБ России и ФСТЭК России от 31 августа 2010 г. № 416/489 (зарегистрирован Минюстом России 13 октября 2010 г., регистрационный № 18704).

сети;

идентификации и аутентификации пользователей многофункционального межсетевого экрана уровня сети;

фильтрации сетевого трафика;

обнаружению и блокированию компьютерных атак;

обнаружению и блокированию вредоносного программного обеспечения;

доверенной загрузке многофункционального межсетевого экрана уровня сети;

тестированию и контролю целостности многофункционального межсетевого экрана уровня сети;

производительности многофункционального межсетевого экрана уровня сети;

аппаратной платформе многофункционального межсетевого экрана уровня сети;

режимам работы многофункционального межсетевого экрана уровня сети;

регистрации событий безопасности в многофункциональном межсетевом экране уровня сети;

обеспечению бесперебойного функционирования и восстановления многофункционального межсетевого экрана уровня сети;

взаимодействию с иными средствами защиты информации;

централизованному и удаленному управлению многофункциональным межсетевым экраном уровня сети.

6. Многофункциональный межсетевой экран уровня сети должен соответствовать Требованиям по безопасности информации, устанавливающим уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий, утвержденным приказом ФСТЭК России от 2 июня 2020 г. № 76 (зарегистрирован Минюстом России 11 сентября 2020 г., регистрационный № 59772) (с изменениями, внесенными приказом ФСТЭК России от 18 апреля 2022 г. № 68 (зарегистрирован Минюстом России 20 июля 2022 г., регистрационный № 69318).

Устанавливается следующее соответствие классов защиты многофункциональных межсетевых экранов уровня сети уровням доверия:

многофункциональные межсетевые экраны уровня сети 6 класса защиты должны соответствовать 6 уровню доверия;

многофункциональные межсетевые экраны уровня сети 5 класса защиты должны соответствовать 5 уровню доверия;

многофункциональные межсетевые экраны уровня сети 4 класса защиты должны соответствовать 4 уровню доверия.

7. К управлению доступом в многофункциональном межсетевом экране уровня сети 6, 5, 4 классов защиты предъявляются следующие требования:

7.1. В многофункциональном межсетевом экране уровня сети 6, 5, 4 классов защиты должен быть реализован ролевой метод управления доступом с тремя ролями пользователей многофункционального межсетевого экрана уровня сети: администратор безопасности, администратор многофункционального межсетевого экрана уровня сети, администратор информационной (автоматизированной) системы.

7.2. Многофункциональный межсетевой экран уровня сети 6, 5, 4 классов защиты должен реализовывать возможность наделения администратора безопасности следующими правами:

выбирать события безопасности, подлежащие регистрации в журнале (журналах) событий безопасности многофункционального межсетевого экрана уровня сети;

осуществлять чтение журнала событий безопасности многофункционального межсетевого экрана уровня сети;

получать оповещения в случае выявления признаков вредоносного программного обеспечения в передаваемых файлах;

получать оповещения в случае выявления сетевого трафика, в котором обнаружен признак компьютерной атаки;

получать оповещения о событиях безопасности;

настраивать параметры выгрузки информации о событиях безопасности, зарегистрированных в многофункциональном межсетевом экране уровня сети;

формировать отчеты с учетом заданных критериев отбора, выгрузки (экспорта) данных из журнала событий безопасности многофункционального межсетевого экрана уровня сети.

7.3. Многофункциональный межсетевой экран уровня сети 6, 5, 4 классов защиты должен реализовывать возможность наделения администратора многофункционального межсетевого экрана уровня сети следующими правами:

создавать учетные записи других пользователей многофункционального межсетевого экрана уровня сети;

управлять учетными записями пользователей многофункционального межсетевого экрана уровня сети;

назначать полномочия пользователям многофункционального межсетевого экрана уровня сети, определяемые их ролями;

устанавливать правила фильтрации, позволяющие настроить разрешение или запрет (блокирование) прохождения сетевого трафика с использованием атрибутов фильтрации сетевого трафика;

устанавливать правила фильтрации, позволяющие настроить разрешение

или запрет (блокирование) прохождения сетевого трафика с использованием атрибутов фильтрации сетевого трафика, а также результатов обнаружения компьютерных атак и вредоносного программного обеспечения;

изменять и удалять правила фильтрации многофункционального межсетевого экрана уровня сети;

применять правила фильтрации к сетевым интерфейсам многофункционального межсетевого экрана уровня сети;

применять правила фильтрации к идентифицированным многофункциональным межсетевым экраном уровня сети пользователям информационной (автоматизированной) системы;

применять правила фильтрации к идентифицированным многофункциональным межсетевым экраном уровня сети приложениям, используемым при сетевом взаимодействии;

управлять приоритетами применения правил фильтрации;

включать и отключать отдельные правила фильтрации при настройке анализа сетевого трафика на наличие признаков компьютерных атак;

устанавливать собственные правила фильтрации при настройке анализа сетевого трафика на наличие признаков компьютерных атак;

осуществлять чтение журнала событий безопасности многофункционального межсетевого экрана уровня сети;

получать оповещения о событиях безопасности;

управлять режимами работы многофункционального межсетевого экрана уровня сети;

изменять конфигурацию многофункционального межсетевого экрана уровня сети;

обновлять программное обеспечение многофункционального межсетевого экрана уровня сети;

тестировать многофункциональный межсетевой экран уровня сети.

7.4. Многофункциональный межсетевой экран уровня сети 6, 5, 4 классов защиты должен реализовывать возможность наделения администратора информационной (автоматизированной) системы правами по управлению параметрами настройки сетевого взаимодействия пользователей многофункционального межсетевого экрана уровня сети, субъектов доступа, пользователей информационной (автоматизированной) системы и устройств через многофункциональный межсетевой экран уровня сети и с многофункциональным межсетевым экраном уровня сети с учетом правил фильтрации.

7.5. Многофункциональный межсетевой экран уровня сети должен реализовывать возможность определения полномочий для пользователей

многофункционального межсетевого экрана уровня сети в пределах назначенных им ролей.

8. К идентификации и аутентификации пользователей многофункционального межсетевого экрана уровня сети предъявляются следующие требования:

8.1. Первичная идентификация пользователей многофункционального межсетевого экрана уровня сети 6 класса защиты должна осуществляться администратором многофункционального межсетевого экрана уровня сети.

Идентификация и аутентификация пользователей многофункционального межсетевого экрана уровня сети осуществляется в соответствии с требованиями раздела 3 ГОСТ Р 58833-2020 «Защита информации. Идентификация и аутентификация. Общие положения»[7].

В случае неуспешной идентификации и аутентификации пользователя многофункционального межсетевого экрана уровня сети ему должно быть отказано в доступе в многофункциональный межсетевой экран уровня сети.

Многофункциональный межсетевой экран уровня сети должен осуществлять аутентификацию пользователей многофункционального межсетевого экрана уровня сети при предъявлении идентификатора и пароля пользователя многофункционального межсетевого экрана уровня сети.

Пароль пользователя многофункционального межсетевого экрана уровня сети для первичной аутентификации должен устанавливаться администратором многофункционального межсетевого экрана уровня сети.

Многофункциональный межсетевой экран уровня сети должен реализовывать возможность изменения пользователем многофункционального межсетевого экрана уровня сети установленного пароля после его первичной аутентификации.

Многофункциональный межсетевой экран уровня сети не должен реализовывать возможность установления одинаковых идентификаторов для разных пользователей многофункционального межсетевого экрана уровня сети.

При попытке ввода неправильного значения идентификатора или пароля пользователя многофункционального межсетевого экрана уровня сети должно выводиться сообщение на экран средства вычислительной техники пользователя с приглашением ввести правильный идентификатор и пароль еще раз.

При исчерпании установленного максимального количества неуспешных попыток ввода неправильного пароля учетная запись пользователя многофункционального межсетевого экрана уровня сети должна быть заблокирована многофункциональным межсетевым экраном уровня сети с

---

[7] Утвержден и введен в действие приказом Федерального агентства по техническому регулированию и метрологии от 10 апреля 2020 г. № 159-ст (М., «Стандартинформ», 2020).

возможностью её разблокировки администратором многофункционального межсетевого экрана уровня сети или автоматически по истечении временного интервала, устанавливаемого администратором многофункционального межсетевого экрана уровня сети.

Защита пароля пользователя многофункционального межсетевого экрана уровня сети должна обеспечиваться при его вводе за счет исключения отображения символов вводимого пароля или за счет отображения вводимых символов условными знаками.

Пароль пользователя многофункционального межсетевого экрана уровня сети 6 класса защиты должен содержать не менее 6 символов при алфавите пароля не менее 60 символов. Максимальное количество попыток ввода неправильного пароля до блокировки – 10.

Многофункциональный межсетевой экран уровня сети должен реализовывать возможность хранения аутентификационной информации пользователя многофункционального межсетевого экрана уровня сети в защищенном от несанкционированного доступа виде.

8.2. Пароль пользователя многофункционального межсетевого экрана уровня сети 5 класса защиты наряду с требованиями, установленными подпунктом 8.1 пункта 8 настоящих Требований, дополнительно должен содержать не менее 6 символов при алфавите пароля не менее 70 символов. Максимальное количество попыток ввода неправильного пароля до блокировки – 8.

Многофункциональный межсетевой экран уровня сети 5 класса защиты должен обеспечивать взаимную идентификацию и аутентификацию пользователей многофункционального межсетевого экрана уровня сети и многофункционального межсетевого экрана уровня сети при удаленном доступе с использованием сетей связи общего пользования.

8.3. Пароль пользователя многофункционального межсетевого экрана уровня сети 4 класса защиты наряду с требованиями, установленными подпунктами 8.1 и 8.2 пункта 8 настоящих Требований, дополнительно должен содержать не менее 8 символов при алфавите пароля не менее 70 символов. Максимальное количество попыток ввода неправильного пароля до блокировки – 4.

9. К фильтрации сетевого трафика многофункциональным межсетевым экраном уровня сети предъявляются следующие требования:

9.1. Многофункциональный межсетевой экран уровня сети 6 класса защиты должен реализовывать возможность:

формирования правил фильтрации сетевого трафика;

фильтрации сетевого трафика, проходящего через многофункциональный

межсетевой экран уровня сети, на основе сформированных правил фильтрации сетевого трафика.

Многофункциональный межсетевой экран уровня сети должен предоставлять возможность создания правил фильтрации для определения разрешения или запрета (блокировки) прохождения сетевого трафика или сетевых пакетов на основе следующих атрибутов:

идентификаторы сетевых интерфейсов (идентификаторы физических сетевых интерфейсов и идентификаторы логических сетевых интерфейсов, которые присваиваются физическим интерфейсам или группам физических сетевых интерфейсов многофункционального межсетевого экрана уровня сети);

сетевые адреса отправителей и (или) получателей сетевого трафика, определяемые из заголовков протокола сетевого уровня;

доменные имена отправителей и (или) получателей сетевого трафика, определяемые из заголовков протокола получения информации о доменах или на основании данных от серверов доменных имен информационной (автоматизированной) системы;

данные о географической принадлежности отправителей и (или) получателей сетевого трафика, определяемые на основе сопоставления используемого им сетевого адреса с базой геоданных многофункционального межсетевого экрана уровня сети, обеспечиваемой производителем (изготовителем) и содержащей сетевые адреса (диапазоны сетевых адресов), которые распределены организациями, занимающимися вопросами адресации и маршрутизации в сетях связи общего пользования и международного информационного обмена, и как минимум, соответствующие им названия и (или) коды стран, а также регионов и (или) городов, которые определяют месторасположение владельцев сетевых адресов;

протокол, используемый для передачи сетевого трафика на сетевом, транспортном и прикладном уровнях взаимодействия сетевых устройств, операционных систем и сетевого программного обеспечения (приложений) информационной (автоматизированной) системы;

двоичные флаги (кодовые биты) управления сетевым соединением и размером отправляемых (получаемых) порций данных из заголовков протокола управления передачей информации на транспортном уровне;

приложение или категория приложения (группа приложений, обладающих общими свойствами, признаками, связями, атрибутами), определяемое (определяемая) на прикладном уровне методом, который основан на поиске в анализируемом сетевом трафике конкретных наборов данных, символов (сигнатур), которые связаны с идентифицируемым приложением;

унифицированный (единообразный) идентификатор информационного

ресурса, определяемый из заголовков протоколов прикладного уровня;

информационный ресурс, с которым связано сетевое взаимодействие, определяемый с использованием базы унифицированных (единообразных) идентификаторов информационных ресурсов и (или) методом, который основан на поиске в анализируемом сетевом трафике конкретных наборов данных, символов (сигнатур), связанных с идентифицируемым ресурсом;

тип передаваемого (загружаемого) файла, содержащегося в сетевом трафике;

тип передаваемого (загружаемого) от веб-страниц информационного объекта, содержащего нежелательную информацию;

тип контента, содержащийся в информационном ресурсе.

Категории приложений, категории информационных ресурсов, типы передаваемых (загружаемых) файлов, типы передаваемых (загружаемых) от веб-страниц информационных объектов, а также типы контента, на основании которых многофункциональный межсетевой экран уровня сети может обеспечивать фильтрацию сетевого трафика, должны быть определены производителем (изготовителем) в руководстве администратора многофункционального межсетевого экрана уровня сети и в технических условиях.

Многофункциональный межсетевой экран уровня сети должен предоставлять возможность включения, отключения, редактирования и удаления созданных правил фильтрации.

Многофункциональный межсетевой экран уровня сети должен предоставлять возможность задания, как минимум, следующих режимов выполнения правил фильтрации:

включение (отключение) правил фильтрации администратором многофункционального межсетевого экрана уровня сети;

включение (отключение) правил фильтрации по расписанию и (или) фильтрации на ограниченный период времени.

Многофункциональный межсетевой экран уровня сети должен предоставлять возможность фильтрации по атрибутам, характеризующим отправителей и получателей сетевого трафика, отслеживаемого на основании сетевых адресов, номеров портов, флагов (признаков) фрагментации, состава двоичных флагов (кодовых битов), позволяющего контролировать входящие и исходящие пакеты на аномалии сетевого соединения.

Многофункциональный межсетевой экран уровня сети должен реализовывать возможность извлекать из сетевых пакетов данные, инкапсулированные в преобразованном (кодированном) виде. Перечень протоколов (алгоритмов) преобразования (кодирования) данных, для которых

многофункциональным межсетевым экраном уровня сети обеспечивается возможность извлечения преобразованных (закодированных) данных из сетевых пакетов, должен быть приведен в руководстве администратора многофункционального межсетевого экрана уровня сети и технических условиях. По отношению к извлеченным данным должны применяться правила фильтрации, настроенные на многофункциональном межсетевом экране уровня сети.

Многофункциональный межсетевой экран уровня сети должен предоставлять возможность блокирования сетевых пакетов, в которые инкапсулированы данные в преобразованном (закодированном) виде с использованием протоколов (алгоритмов), для которых многофункциональным межсетевым экраном уровня сети не обеспечивается возможность извлечения преобразованных (закодированных) данных из сетевых пакетов.

9.2. Многофункциональный межсетевой экран уровня сети 5 класса защиты наряду с требованиями, установленными в подпункте 9.1 пункта 9 настоящих Требований, дополнительно должен предоставлять возможность создания правил фильтрации для определения разрешения или запрета (блокирования) прохождения сетевого трафика или сетевых пакетов на основе следующих атрибутов:

логическое имя пользователя информационной (автоматизированной) системы, связанное с идентификатором учетной записи (идентификатор учетной записи, идентификатор группы учетных записей, идентификатор универсальных групп (встроенных групп учетных записей операционных систем) или универсальной учетной записи (встроенных учетных записей операционных систем);

идентификатор веб-клиента (набор атрибутов веб-клиента), определяемый из заголовка в протоколе передачи гипертекста;

веб-методы (способы) обмена данными веб-клиента с веб-сервером, определяемые из заголовка протокола передачи гипертекста.

Многофункциональный межсетевой экран уровня сети должен предоставлять, как минимум, следующие методы сопоставления логического имени субъекта доступа с сетевым адресом:

указание администратором многофункционального межсетевого экрана уровня сети принадлежности сетевого адреса к логическому имени пользователя информационной (автоматизированной) системы (создание, изменение администратором таблицы сопоставления);

получение списка идентификаторов пользователей информационной (автоматизированной) системы и (или) связанных с ними идентификаторов учетных записей, а также сетевых адресов устройств, с которых выполнена

авторизация этих субъектов доступа из информационной (автоматизированной) системы;

авторизация пользователей информационной (автоматизированной) системы по сети в информационной (автоматизированной) системе через специальную веб-страницу (форму), предоставляемую многофункциональным межсетевым экраном уровня сети, в процессе которой сетевой адрес определяется из отправляемого пользователем информационной (автоматизированной) системы сетевого трафика, а подлинность логического имени, указываемого пользователем информационной (автоматизированной) системы в веб-странице, подтверждается в информационной (автоматизированной) системе.

9.3. Многофункциональный межсетевой экран уровня сети 4 класса защиты наряду с требованиями, установленными в подпунктах 9.1 и 9.2 пункта 9 настоящих Требований, дополнительно должен предоставлять возможность создания правил фильтрации для определения разрешения или запрета (блокирования) прохождения сетевого трафика или сетевых кадров на основе следующих атрибутов:

действительный сетевой адрес субъекта доступа, осуществляющего передачу сетевого трафика через прокси-сервер из специального заголовка протокола передачи гипертекста;

физические адреса отправителей и (или) получателей сетевого трафика, определяемые из заголовков протокола канального уровня.

Многофункциональный межсетевой экран уровня сети самостоятельно или с применением сертифицированных средств защиты информации от ее утечки из информационной (автоматизированной) системы дополнительно должен определять тип контента, содержащегося в информационной (автоматизированной) системе и в проходящем через многофункциональный межсетевой экран уровня сети сетевом трафике, методом морфологического анализа информации, который основывается на применении морфологических словарей, содержащих словарные формы лексем и соответствующий им тип контента. В многофункциональном межсетевом экране уровня сети или в применяемом с ним сертифицированном средстве защиты информации от ее утечки из информационной (автоматизированной) системы должна быть реализована возможность создания типов контента и словарных форм лексем и (или) морфологических словарей.

10. К обнаружению и блокированию компьютерных атак в многофункциональном межсетевом экране уровня сети предъявляются следующие требования:

10.1. Многофункциональный межсетевой экран уровня сети 6, 5 классов

защиты самостоятельно или с применением включенной в его состав сертифицированной системы обнаружения вторжений должен:

обнаруживать признаки компьютерных атак в проходящем через многофункциональный межсетевой экран уровня сети сетевом трафике на основе базы решающих правил;

блокировать сетевой трафик, в котором обнаружены признаки компьютерной атаки;

обеспечивать обновление базы решающих правил.

Многофункциональный межсетевой экран уровня сети 6, 5 классов защиты должен реализовывать возможность обнаружения:

атак сетевого сканирования;

атак проникновения, связанных с эксплуатацией уязвимостей информационной (автоматизированной) системы;

атак, направленных на отказ в обслуживании;

атак подбора аутентификационной информации.

10.2. Многофункциональный межсетевой экран уровня сети 4 класса защиты наряду с требованиями, установленными в подпункте 10.1 пункта 10 настоящих Требований, дополнительно должен реализовывать возможность при обращении субъекта доступа по доменному имени к информационному ресурсу проверять этот ресурс на наличие связей с потенциально небезопасными информационными ресурсами.

Наличие связи с потенциально небезопасными информационными ресурсами проверяется одним из следующих способов:

проверка наличия сведений о том, что информационный ресурс является потенциально небезопасным в предоставляемых разработчиком многофункционального межсетевого экрана уровня сети базах данных, содержащих консолидированные из различных источников сведения об угрозах безопасности информации;

тестовое обращение к информационному ресурсу из входящей в состав многофункционального межсетевого экрана уровня сети или применяемой совместно с ним сертифицированной изолированной замкнутой системы (среды) предварительного выполнения программ для проверки действий, осуществляемых со стороны информационного ресурса, в этой изолированной системе (среде) предварительного выполнения программ на наличие признаков вредоносной активности.

Многофункциональный межсетевой экран уровня сети должен обладать возможностью блокировать сетевой трафик, в котором обнаружена гиперссылка, связанная с потенциально небезопасным информационным ресурсом.

11. К обнаружению и блокированию вредоносного программного

обеспечения в многофункциональном межсетевом экране уровня сети предъявляются следующие требования:

11.1. Многофункциональный межсетевой экран уровня сети 6, 5 классов защиты должен:

обнаруживать признаки вредоносного программного обеспечения в проходящем через многофункциональный межсетевой экран уровня сети сетевом трафике на основе базы данных признаков вредоносного программного обеспечения;

блокировать сетевой трафик, в котором обнаружены признаки вредоносного программного обеспечения на основе базы данных признаков вредоносного программного обеспечения;

обеспечивать обновление базы данных признаков вредоносного программного обеспечения.

11.2. Многофункциональный межсетевой экран уровня сети 4 класса защиты наряду с требованиями, установленными в подпункте 11.1 пункта 11 настоящих Требований, дополнительно должен реализовывать возможность проверки файлов, передаваемых в сетевом трафике, во входящей в состав многофункционального межсетевого экрана уровня сети или применяемой совместно с ним сертифицированной среде предварительного выполнения программ (обращения к объектам файловой системы) на наличие признаков вредоносного программного обеспечения.

Проверка файла, передаваемого в сетевом трафике, на наличие признаков вредоносного программного обеспечения должна осуществляться путем запуска его в изолированной от информационной (автоматизированной) системы замкнутой системе (среде) предварительного выполнения программ и проверки его действий в операционной системе, в файловой системе и оперативной памяти на наличие признаков вредоносной активности.

12. К доверенной загрузке многофункционального межсетевого экрана уровня сети предъявляются следующие требования:

12.1. В составе многофункционального межсетевого экрана уровня сети 6 класса защиты должно применяться средство доверенной загрузки 6 класса защиты, соответствующее Требованиям к средствам доверенной загрузки, утвержденным приказом ФСТЭК России от 27 сентября 2013 г. № 119 (зарегистрирован Минюстом России 16 декабря 2013 г., регистрационный № 30604).

12.2. В составе многофункционального межсетевого экрана уровня сети 5 класса защиты должно применяться средство доверенной загрузки 5 класса защиты, соответствующее Требованиям к средствам доверенной загрузки, утвержденным приказом ФСТЭК России от 27 сентября 2013 г. № 119.

12.3. В составе многофункционального межсетевого экрана уровня сети 4 класса защиты должно применяться средство доверенной загрузки 4 класса защиты, соответствующее Требованиям к средствам доверенной загрузки, утвержденным приказом ФСТЭК России от 27 сентября 2013 г. № 119.

13. К тестированию и контролю целостности в многофункциональном межсетевом экране уровня сети предъявляются следующие требования:

13.1. Многофункциональный межсетевой экран уровня сети 6, 5 классов защиты должен:

обеспечить по запросу администратора многофункционального межсетевого экрана уровня сети тестирование правильности выполнения функции фильтрации сетевого трафика;

обеспечивать возможность блокировки проходящего через него сетевого трафика, если по результатам тестирования функций фильтрации сетевого трафика будет выявлено нарушение их функционирования;

информировать администратора многофункционального межсетевого экрана уровня сети о выявленных нарушениях функционирования функций фильтрации сетевого трафика.

13.2. Многофункциональный межсетевой экран уровня сети 4 класса защиты наряду с требованиями, установленными в подпунктах 13.1 и 13.2 пункта 13 настоящих Требований, дополнительно должен:

содержать встроенный программно-аппаратный модуль, обеспечивающий целостность встроенного программного обеспечения аппаратной платформы многофункционального межсетевого экрана уровня сети, реализующего функции базовой системы ввода-вывода (загрузчика операционной среды) и функции безопасности многофункционального межсетевого экрана уровня сети, для которого не может быть исключена возможность перезаписи без использования средств разработки;

информировать администратора многофункционального межсетевого экрана уровня сети о нарушении целостности программного обеспечения.

14. К производительности многофункционального межсетевого экрана уровня сети предъявляются следующие требования:

В формуляре многофункционального межсетевого экрана уровня сети 6, 5, 4 классов защиты должны быть указаны подтверждаемые в соответствии с методикой производителя (изготовителя) сведения:

о пропускной способности многофункционального межсетевого экрана уровня сети и задержках сетевых пакетов (кадров) в режиме пакетной фильтрации трафика, содержащего сетевые кадры размером 1518 байт и отдельно 64 байта;

о пропускной способности многофункционального межсетевого экрана

уровня сети и задержках сетевых пакетов (кадров) веб-трафика в определенных производителем (изготовителем) комбинациях включённых функций безопасности;

о количестве экземпляров многофункционального межсетевого экрана уровня сети, которые могут совместно работать в режиме балансировки нагрузки, и их общей пропускной способности.

Производитель (изготовитель) должен определить в формуляре максимальное количество устанавливаемых сетевых соединений в секунду и максимальное количество включенных правил фильтрации, при которых достигаются определенные показатели.

В формуляре многофункционального межсетевого экрана уровня сети должны быть указаны сведения о способе балансировки нагрузки и (или) используемом средстве (используемых средствах) балансировки нагрузки.

15. К аппаратной платформе многофункционального межсетевого экрана уровня сети предъявляются следующие требования:

15.1. Аппаратная платформа многофункционального межсетевого экрана уровня сети 6 класса защиты должна ограничивать доступ через сетевые интерфейсы к оперативной памяти только в разрешенном диапазоне адресов и исключать возможность доступа (как на чтение, так и на запись) к остальной части оперативной памяти аппаратной платформы со стороны сетевого интерфейса.

При разработке многофункционального межсетевого экрана уровня сети интерфейс, через который осуществляется управление многофункциональным межсетевым экраном уровня сети, должен рассматриваться разработчиком многофункционального межсетевого экрана уровня сети как интерфейс функций безопасности.

В рамках испытаний многофункционального межсетевого экрана уровня сети изготовителем многофункционального межсетевого экрана уровня сети должно быть доказано, что субъектам доступа, пользователям информационной (автоматизированной) системы и устройствам, осуществляющим передачу информационных потоков через многофункциональный межсетевой экран уровня сети, не может быть доступен интерфейс функций управления многофункциональным межсетевым экраном уровня сети и сетевой трафик, поступающий в многофункциональный межсетевой экран уровня сети от пользователей многофункционального межсетевого экрана уровня сети, осуществляющих управление многофункциональным межсетевым экраном уровня сети.

15.2. Аппаратная платформа многофункционального межсетевого экрана уровня сети 5 класса защиты наряду с требованиями, установленными в

подпункте 15.1 пункта 15 настоящих Требований, дополнительно должна содержать компоненты, на аппаратном уровне реализующие пакетную фильтрацию на основе сетевых адресов отправителей и (или) получателей сетевого трафика. Наличие или отсутствие в многофункциональном межсетевом экране уровня сети компонентов, на аппаратном уровне реализующих пакетную фильтрацию сетевого трафика, указывается в формуляре многофункционального межсетевого экрана уровня сети.

15.3. Аппаратная платформа многофункционального межсетевого экрана уровня сети 4 класса защиты наряду с требованиями, установленными в подпунктах 15.1 и 15.2 пункта 15 настоящих Требований, дополнительно должна содержать компоненты, на аппаратном уровне реализующие пакетную фильтрацию на основе физических адресов отправителей и (или) получателей сетевого трафика.

16. К режимам работы многофункционального межсетевого экрана уровня сети предъявляются следующие требования:

16.1. Многофункциональный межсетевой экран уровня сети 6, 5 классов защиты должен реализовывать возможность работы в следующих режимах:

режим, при котором блокируется весь входящий, исходящий сетевой трафик, проходящий через многофункциональный межсетевой экран уровня сети;

режим, при котором разрешены сетевые потоки, не запрещённые включенными запрещающими (блокирующими) правилами фильтрации (в данном режиме среди множества неразрешенных сетевых потоков отдельные потоки могут разрешаться);

режим, при котором разрешены только разрешенные включенными разрешающими правилами фильтрации сетевые потоки (в данном режиме среди множества разрешенных сетевых потоков отдельные потоки могут блокироваться включенными запрещающими (блокирующими) правилами фильтрации).

16.2. Многофункциональный межсетевой экран уровня сети 4 класса защиты наряду с требованиями, установленными в подпункте 16.1 пункта 16 настоящих Требований, дополнительно должен реализовывать возможность работы в следующих режимах:

режим репликации проходящих через многофункциональный межсетевой экран уровня сети данных, извлеченных из сетевых пакетов, в которых информация инкапсулирована в преобразованном (кодированном) по определенным алгоритмам виде, во внешнее программное или программно-аппаратное средство для дополнительного анализа;

режим промежуточного сервера приложений, при котором доступ

субъектов доступа, пользователей информационной (автоматизированной) системы и устройств к информационным ресурсам осуществляется от имени многофункционального межсетевого экрана уровня сети путем установления двух отдельных соединений: первое – между субъектом доступа и многофункциональным межсетевым экраном уровня сети, второе – между многофункциональным межсетевым экраном уровня сети и объектом доступа.

Многофункциональный межсетевой экран уровня сети в режиме промежуточного сервера приложений должен реализовывать возможность взаимодействия авторизованным на многофункциональном межсетевом экране уровня сети пользователям информационной (автоматизированной) системы и (или) устройствам информационной (автоматизированной) системы с информационными ресурсами сети связи общего пользования без раскрытия сетевого адреса устройства.

Многофункциональный межсетевой экран уровня сети должен работать в режиме промежуточного сервера для протокола передачи гипертекста. Перечень протоколов, для которых многофункциональный межсетевой экран уровня сети работает в режиме промежуточного сервера, должен быть указан производителем (изготовителем) в руководстве администратора многофункционального межсетевого экрана уровня сети и технических условиях.

17. К регистрации событий безопасности в многофункциональном межсетевом экране уровня сети предъявляются следующие требования:

17.1. Многофункциональный межсетевой экран уровня сети 6, 5 классов защиты должен обеспечивать:

регистрацию выбранных администратором безопасности событий безопасности в журнале (журналах) событий безопасности многофункционального межсетевого экрана уровня сети;

предоставление возможности просмотра всех событий безопасности в журнале (журналах) событий безопасности многофункционального межсетевого экрана уровня сети и выборочного просмотра событий безопасности (поиск, сортировка событий безопасности) в соответствии с ролью пользователя многофункционального межсетевого экрана уровня сети.

Многофункциональный межсетевой экран уровня сети должен реализовывать возможность регистрации следующих типов событий безопасности в соответствии с разделами 3 - 6 ГОСТ Р 59548 «Защита информации. Регистрация событий безопасности. Требования к регистрируемой информации» [8]:

---

[8] Утвержден и введен в действие приказом Федерального агентства по техническому регулированию и метрологии от 13 января 2022 г. № 2-ст (М., «Стандартинформ», 2022).

события безопасности, связанные с фильтрацией сетевого трафика;

события безопасности, связанные с обнаружением признаков вредоносного программного обеспечения в сетевом трафике;

события безопасности, связанные с обнаружением признаков компьютерных атак в сетевом трафике;

события безопасности, связанные с идентификацией и аутентификацией пользователя многофункционального межсетевого экрана уровня сети;

события безопасности, связанные с управлением (администрированием) многофункционального межсетевого экрана уровня сети;

события безопасности, связанные с управлением журналами событий безопасности;

события безопасности, связанные с контролем целостности программного обеспечения многофункционального межсетевого экрана уровня сети;

события безопасности, связанные со сбоями в работе многофункционального межсетевого экрана уровня сети.

Многофункциональный межсетевой экран уровня сети должен реализовывать возможность хранения журналов событий безопасности с возможностью ротации событий безопасности (запись новых событий безопасности взамен старых).

Многофункциональный межсетевой экран уровня сети при записи событий безопасности информации должен получать информацию о текущей дате, времени и часовом поясе от системных часов многофункционального межсетевого экрана уровня сети, которые должны иметь возможность синхронизации информации о текущей дате и времени с сервером единого времени, располагаемым в информационной (автоматизированной) системе, и (или) с часами, функционирующими в аппаратной платформе многофункционального межсетевого экрана уровня сети.

Многофункциональный межсетевой экран уровня сети должен оповещать пользователей многофункционального межсетевого экрана уровня сети о событиях безопасности в соответствии с ролями пользователей многофункционального межсетевого экрана уровня сети.

17.2. Многофункциональный межсетевой экран уровня сети 4 класса защиты наряду с требованиями, установленными в подпункте 17.1 пункта 17 настоящих Требований, дополнительно должен регистрировать события безопасности при работе в режиме промежуточного сервера приложений с указанием в параметрах регистрации действительных идентификаторов отправителей и получателей сетевого трафика (используемые сетевые и физические адреса, используемые сетевые порты).

18. К обеспечению бесперебойного функционирования и восстановления

многофункционального межсетевого экрана уровня сети предъявляются следующие требования:

18.1. Многофункциональный межсетевой экран уровня сети 6 класса защиты должен:

сохранять параметры настройки, которые могут использоваться для восстановления в случаях выхода многофункционального межсетевого экрана уровня сети из строя (параметры учетных записей, параметры настройки сетевых интерфейсов, правила фильтрации сетевого трафика, параметры настройки базы решающих правил и базы данных признаков вредоносных компьютерных программ);

обеспечивать восстановление параметров настройки многофункционального межсетевого экрана уровня сети на другом экземпляре многофункционального межсетевого экрана уровня сети.

18.2. Многофункциональный межсетевой экран уровня сети 5 класса защиты наряду с требованиями, установленными в подпункте 18.1 пункта 18 настоящих Требований, дополнительно должен обеспечивать возможность работы в отказоустойчивом кластере.

Параметры настройки конфигурации устройств кластера многофункционального межсетевого экрана уровня сети должны синхронизироваться.

В случае отказа основного устройства кластера многофункционального межсетевого экрана уровня сети резервное устройство кластера должно взять на себя все функции по обработке сетевого трафика в соответствии с конфигурацией устройств кластера без прерывания сетевых сессий.

В многофункциональном межсетевом экране уровня сети должна обеспечиваться возможность поочередного обновления программного обеспечения каждого устройства кластера без прерывания функций безопасности многофункционального межсетевого экрана уровня сети.

При неуспешном обновлении программного обеспечения многофункционального межсетевого экрана уровня сети должна обеспечиваться возможность возврата к предыдущему состоянию без прерывания функций безопасности многофункционального межсетевого экрана уровня сети и без прерывания работы кластера.

Компьютерные атаки, направленные на отказ в обслуживании, содержащиеся в транзитном сетевом трафике, не должны приводить к недоступности интерфейса управления многофункциональным межсетевым экраном уровня сети.

18.3. Многофункциональный межсетевой экран уровня сети 4 класса защиты наряду с требованиями, установленными в подпунктах 18.1 и 18.2 пункта

18 настоящих Требований, дополнительно должен обеспечивать возможность восстановления (для предусмотренных сценариев сбоев программного обеспечения многофункционального межсетевого экрана уровня сети и журнала событий безопасности многофункционального межсетевого экрана уровня сети) штатного функционирования многофункционального межсетевого экрана уровня сети.

19. К взаимодействию с иными средствами защиты информации в многофункциональном межсетевом экране уровня сети предъявляются следующие требования.

Многофункциональный межсетевой экран уровня сети 6, 5, 4 классов защиты должен обеспечивать возможность передавать зарегистрированные им события безопасности в систему управления событиями безопасности информации.

Многофункциональный межсетевой экран уровня сети может осуществлять взаимодействие со средствами защиты информации от ее утечки из информационной (автоматизированной) системы и другими средствами защиты информации в информационной (автоматизированной) системе.

Для взаимодействия многофункционального межсетевого экрана уровня сети со средствами защиты информации должны использоваться выделенные физические и (или) логические каналы связи.

20. В состав многофункционального межсетевого экрана уровня сети 5, 4 классов защиты должны входить компоненты, обеспечивающие возможность централизованного управления несколькими экземплярами многофункциональных межсетевых экранов уровня сети, эксплуатируемых в одной информационной (автоматизированной) системе, в соответствии с ролями пользователей многофункциональных межсетевых экранов уровня сети.

В случае осуществления удаленного доступа к многофункциональному межсетевому экрану уровня сети от имени пользователей многофункционального межсетевого экрана уровня сети защита информации должна обеспечиваться путем защиты каналов связи от несанкционированного физического доступа (подключения) к ним и (или) иными методами.