ГОСУДАРСТВЕННАЯ ТЕХНИЧЕСКАЯ КОМИССИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Руководящий документ

СРЕДСТВА ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ. МЕЖСЕТЕВЫЕ ЭКРАНЫ. ЗАЩИТА ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА К ИНФОРМАЦИИ. ПОКАЗАТЕЛИ ЗАЩИЩЕННОСТИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА К ИНФОРМАЦИИ

Москва – 1997

Руководящий документ Гостехкомиссии России «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации». – М.: ГТК РФ, 1997. – 18 с.

Настоящий руководящий документ устанавливает классификацию межсетевых экранов (МЭ) по уровню защищенности от несанкционированного доступа (НСД) к информации на базе перечня показателей защищенности и совокупности описывающих их требований.

Под сетями ЭВМ, распределенными автоматизированными системами (АС) в данном документе понимаются соединенные каналами связи системы обработки данных, ориентированные на конкретного пользователя.

МЭ представляет собой локальное (однокомпонентное) или функционально-распределенное средство (комплекс), реализующее контроль за информацией, поступающей в АС и/или выходящей из АС, и обеспечивает защиту АС посредством фильтрации информации, т.е. ее анализа по совокупности критериев и принятия решения о ее распространении в (из) АС.

Руководящий документ разработан в дополнение к Руководящим документам Гостехкомиссии России “Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации” и “Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации”.

Документ предназначен для заказчиков и разработчиков МЭ, а также сетей ЭВМ, распределенных автоматизированных систем с целью использования при формулировании и реализации требований по их защите от НСД к информации.

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Данные показатели содержат требования к средствам защиты, обеспечивающим безопасное взаимодействие сетей ЭВМ, АС посредством управления межсетевыми потоками информации, и реализованных в виде МЭ.

1.2. Показатели защищенности применяются к МЭ для определения уровня защищенности, который они обеспечивают при межсетевом взаимодействии.

Конкретные перечни показателей определяют классы защищенности МЭ.

1.3. Деление МЭ на соответствующие классы по уровням контроля межсетевых информационных потоков с точки зрения защиты информации необходимо в целях разработки и применения обоснованных и экономически оправданных мер по достижению требуемого уровня защиты информации при взаимодействии сетей ЭВМ, АС.

1.4. Дифференциация подхода к выбору функций защиты в МЭ определяется АС, для защиты которой применяется данный экран.

1.5. Устанавливается пять классов защищенности МЭ.

Каждый класс характеризуется определенной минимальной совокупностью требований по защите информации.

Самый низкий класс защищенности - пятый, применяемый для безопасного взаимодействия АС класса 1Д с внешней средой, четвертый - для 1Г, третий - 1В, второй - 1Б, самый высокий - первый, применяемый для безопасного взаимодействия АС класса 1А с внешней средой.

1.6. Требования, предъявляемые к МЭ, не исключают требований, предъявляемых к средствам вычислительной техники (СВТ) и АС в соответствии с руководящими документами Гостехкомиссии России “Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации” и “Автоматизированные

системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации”.

При включении МЭ в АС определенного класса защищенности, класс защищенности совокупной АС, полученной из исходной путем добавления в нее МЭ, не должен понижаться.

Для АС класса 3Б, 2Б должны применяться МЭ не ниже 5 класса.

Для АС класса 3А, 2А в зависимости от важности обрабатываемой информации должны применяться МЭ следующих классов:

при обработке информации с грифом “секретно” - не ниже 3 класса;

при обработке информации с грифом “совершенно секретно” - не ниже 2 класса;

при обработке информации с грифом “особой важности” - не ниже 1 класса.

2. ТРЕБОВАНИЯ К МЕЖСЕТЕВЫМ ЭКРАНАМ

2.1. Показатели защищенности

2.1.1. Перечень показателей по классам защищенности МЭ приведен в таблице.

Обозначения:

« - » - нет требований к данному классу;

« + » - новые или дополнительные требования,

« = » - требования совпадают с требованиями к МЭ предыдущего класса.

Показатели защищенности	**Классы защищенности**				
	5	4	3	2	1
Управление доступом (фильтрация данных и трансляция адресов)	+	+	+	+	=
Идентификация и аутентификация	-	-	+	=	+

Регистрация	-	+	+	+	=
Администрирование: идентификация и аутентификация	+	=	+	+	+
Администрирование: регистрация	+	+	+	=	=
Администрирование: простота использования	-	-	+	=	+
Целостность	+	=	+	+	+
Восстановление	+	=	=	+	=
Тестирование	+	+	+	+	+
Руководство администратора защиты	+	=	=	=	=
Тестовая документация	+	+	+	+	+
Конструкторская (проектная) документация	+	=	+	=	+

2.2. Требования к пятому классу защищенности МЭ.

2.2.1. Управление доступом.

МЭ должен обеспечивать фильтрацию на сетевом уровне.

Решение по фильтрации может приниматься для каждого сетевого пакета независимо на основе, по крайней мере, сетевых адресов отправителя и получателя или на основе других эквивалентных атрибутов.

2.2.2. Администрирование: идентификация и аутентификация.

МЭ должен обеспечивать идентификацию и аутентификацию администратора МЭ при его локальных запросах на доступ. МЭ должен предоставлять возможность для идентификации и аутентификации по идентификатору (коду) и паролю условно-постоянного действия.

2.2.3. Администрирование: регистрация.

МЭ должен обеспечивать регистрацию входа (выхода) администратора МЭ в систему (из системы) либо загрузки и инициализации системы и ее программного останова. Регистрация выхода из системы не проводится в моменты аппаратурного отключения МЭ;

В параметрах регистрации указываются:

дата, время и код регистрируемого события;

результат попытки осуществления регистрируемого события – успешная или неуспешная;

идентификатор администратора МЭ, предъявленный при попытке осуществления регистрируемого события.

2.2.4. Целостность.

МЭ должен содержать средства контроля за целостностью своей программной и информационной части.

2.2.5. Восстановление.

МЭ должен предусматривать процедуру восстановления после сбоев и отказов оборудования, которые должны обеспечивать восстановление свойств МЭ.

2.2.6. Тестирование.

В МЭ должна обеспечиваться возможность регламентного тестирования:

реализации правил фильтрации (см. п. 2.2.1);

процесса идентификации и аутентификации администратора МЭ (см. п. 2.2.2);

процесса регистрации действий администратора МЭ (см. п. 2.2.3.);

процесса контроля за целостностью программной и информационной части МЭ (см. п.2.2.4);

процедуры восстановления (см. п. 2.2.5.).

2.2.7. Руководство администратора МЭ.

Документ содержит:

описание контролируемых функций МЭ;

руководство по настройке и конфигурированию МЭ;

описание старта МЭ и процедур проверки правильности старта;

руководство по процедуре восстановления.

2.2.8. Тестовая документация.

Должна содержать описание тестов и испытаний, которым подвергался МЭ (в соответствии с п. 2.2.6), и результаты тестирования.

2.2.9. Конструкторская (проектная) документация.

Должна содержать:

общую схему МЭ;

общее описание принципов работы МЭ;

описание правил фильтрации;

описание средств и процесса идентификации и аутентификации;

описание средств и процесса регистрации;

описание средств и процесса контроля за целостностью программной и информационной части МЭ;

описание процедуры восстановления свойств МЭ.

2.3. Требования к четвертому классу защищенности МЭ.

2.3.1. Управление доступом.

Данные требования полностью включают аналогичные требования пятого класса (п.2.2.1).

Дополнительно МЭ должен обеспечивать:

фильтрацию пакетов служебных протоколов, служащих для диагностики и управления работой сетевых устройств;

фильтрацию с учетом входного и выходного сетевого интерфейса как средство проверки подлинности сетевых адресов;

фильтрацию с учетом любых значимых полей сетевых пакетов.

2.3.2. Регистрация.

МЭ должен обеспечивать возможность **регистрации и учета фильтруемых пакетов**. **В параметры регистрации включаются адрес, время и результат фильтрации.**

2.3.3. Администрирование: идентификация и аутентификация.

Данные требования полностью совпадают с аналогичными требованиями пятого класса (п.2.2.2).

2.3.4. Администрирование: регистрация.

Данные требования включают аналогичные требования пятого класса (п.2.2.3).

Дополнительно МЭ должен обеспечивать регистрацию запуска программ и процессов (заданий, задач).

2.3.5. Целостность.

Данные требования полностью совпадают с аналогичными требованиями пятого класса (п.2.2.4).

2.3.6. Восстановление.

Данные требования полностью совпадают с аналогичными требованиями пятого класса (п.2.2.5).

2.3.7. Тестирование.

В МЭ должна обеспечиваться возможность регламентного тестирования:

реализации правил фильтрации (см. п. 2.3.1);

процесса регистрации (см. п. 2.3.2);

процесса идентификации и аутентификации администратора МЭ (см. п. 2.3.3);

процесса регистрации действий администратора МЭ (см. п. 2.3.4);

процесса контроля за целостностью программной и информационной части МЭ (см. п.2.3.5);

процедуры восстановления (см. п. 2.3.6).

2.3.8. Руководство администратора МЭ.

Данные требования полностью совпадают с аналогичными требованиями пятого класса (п. 2.2.7).

2.3.9. Тестовая документация.

Должна содержать описание тестов и испытаний, которым подвергался МЭ (в соответствии с п. 2.3.7), и результаты тестирования.

2.3.10. Конструкторская (проектная) документация.

Данные требования полностью совпадают с аналогичными требованиями пятого класса (п. 2.2.9) по составу документации.

2.4. Требования к третьему классу защищенности МЭ.

2.4.1. Управление доступом.

Данные требования полностью включают аналогичные требования четвертого класса (п. 2.3.1).

Дополнительно МЭ должен обеспечивать:

фильтрацию на транспортном уровне запросов на установление виртуальных соединений. При этом, по крайней мере, учитываются транспортные адреса отправителя и получателя;

фильтрацию на прикладном уровне запросов к прикладным сервисам. При этом, по крайней мере, учитываются прикладные адреса отправителя и получателя;

фильтрацию с учетом даты/времени.

2.4.2. Идентификация и аутентификация.

МЭ должен обеспечивать возможность **аутентификации входящих и исходящих запросов методами, устойчивыми к пассивному и/или активному прослушиванию сети**.

2.4.3. Регистрация.

Данные требования включают аналогичные требования четвертого класса (п.2.3.2).

Дополнительно МЭ должен обеспечивать:

регистрацию и учет запросов на установление виртуальных соединений;

локальную сигнализацию попыток нарушения правил фильтрации.

< 2.4.1); п. (см. фильтрации правил реализации процесса регистрации (см. п. 2.4.3);

процесса идентификации и аутентификации запросов (см. п. 2.4.2);

процесса идентификации и аутентификации администратора МЭ (см. п. 2.4.4);

процесса регистрации действий администратора МЭ (см. п. 2.4.5);

процесса контроля за целостностью программной и информационной части МЭ (см. п. 2.4.7);

процедуры восстановления (см. п. 2.4.8.).

2.4.10. Руководство администратора МЭ.

Данные требования полностью совпадают с аналогичными требованиями пятого класса (п.2.2.7).

2.4.11. Тестовая документация.

Должна содержать описание тестов и испытаний, которым подвергался МЭ (в соответствии с п. 2.4.9), и результаты тестирования.

2.4.12. Конструкторская (проектная) документация.

Данные требования полностью включают аналогичные требования пятого класса (п. 2.2.9) по составу документации.

Дополнительно документация должна содержать описание средств и процесса централизованного управления компонентами МЭ.

2.5. Требования ко второму классу защищенности МЭ.

2.5.1. Управление доступом.

Данные требования включают аналогичные требования третьего класса (п.2.4.1).

Дополнительно МЭ должен обеспечивать:

возможность сокрытия субъектов (объектов) и/или прикладных функций защищаемой сети;

возможность трансляции сетевых адресов.

2.5.2. Идентификация и аутентификация.

Данные требования полностью совпадают с аналогичными требованиями третьего класса (п.2.4.2).

2.5.3. Регистрация.

Данные требования включают аналогичные требования третьего класса (п.2.4.3).

Дополнительно МЭ должен обеспечивать:

дистанционную сигнализацию попыток нарушения правил фильтрации;

регистрацию и учет запрашиваемых сервисов прикладного уровня;

программируемую реакцию на события в МЭ.

2.5.4. Администрирование: идентификация и аутентификация.

МЭ должен обеспечивать идентификацию и аутентификацию администратора МЭ при его запросах на доступ. МЭ должен предоставлять возможность для идентификации и аутентификации по идентификатору (коду) и паролю временного действия. МЭ должен препятствовать доступу неидентифицированного субъекта или субъекта, подлинность идентификации которого при аутентификации не подтвердилась.

При удаленных запросах на доступ администратора МЭ идентификация и аутентификация должны обеспечиваться методами, устойчивыми к пассивному и активному перехвату информации.

2.5.5. Администрирование: регистрация.

Данные требования полностью совпадают с аналогичными требованиями третьего класса (п.2.4.5).

2.5.6. Администрирование: простота использования.

Данные требования полностью совпадают с аналогичными требованиями третьего класса (п.2.4.6).

2.5.7. Целостность.

МЭ должен содержать средства контроля за целостностью своей программной и информационной части по контрольным суммам **как в процессе загрузки, так и динамически**.

2.5.8. Восстановление.

МЭ должен предусматривать процедуру восстановления после сбоев и отказов оборудования, которые должны обеспечивать оперативное восстановление свойств МЭ.

2.5.9. Тестирование.

В МЭ должна обеспечиваться возможность регламентного тестирования;

реализации правил фильтрации (см. п. 2.5.1);

процесса идентификации и аутентификации (см. п. 2.5.2);

процесса регистрации (см. п. 2.5.3);

процесса идентификации и аутентификации администратора МЭ (см. п. 2.5.4);

процесса регистрации действий администратора МЭ (см. п. 2.5.5);

процесса контроля за целостностью программной и информационной части МЭ (см. п. 2.5.7);

процедуры восстановления (см. п. 2.5.8).

2.5.10. Руководство администратора МЭ.

Данные требования полностью совпадают с аналогичными требованиями пятого класса (п.2.2.7).

2.5.11. Тестовая документация.

Должна содержать описание тестов и испытаний, которым подвергался МЭ (в соответствии с п. 2.5.9), и результаты тестирования.

2.5.12. Конструкторская (проектная) документация.

Данные требования полностью совпадают с аналогичными требованиями третьего класса (п. 2.4.12) по составу документации.

2.6. Требования к первому классу защищенности МЭ.

2.6.1. Управление доступом.

Данные требования полностью совпадают с аналогичными требованиями второго класса (п.2.5.1).

2.6.2. Идентификация и аутентификация.

Данные требования полностью включают аналогичные требования второго класса (п.2.5.2).

Дополнительно МЭ должен обеспечивать идентификацию и аутентификацию всех субъектов прикладного уровня.

2.6.3. Регистрация.

Данные требования полностью совпадают с аналогичными требованиями второго класса (п.2.5.3).

2.6.4. Администрирование: идентификация и аутентификация.

МЭ должен обеспечивать идентификацию и аутентификацию администратора МЭ при его запросах на доступ. МЭ должен предоставлять возможность для идентификации и аутентификации **по биометрическим характеристикам или специальным устройствам (жетонам, картам, электронным ключам) и паролю временного действия**. МЭ должен препятствовать доступу неидентифицированного субъекта или субъекта, подлинность идентификации которого при аутентификации не подтвердилась.

При удаленных запросах на доступ администратора МЭ идентификация и аутентификация должны обеспечиваться методами, устойчивыми к пассивному и активному перехвату информации.

2.6.5. Администрирование: регистрация.

Данные требования полностью совпадают с аналогичными требованиями третьего класса (п.2.4.5).

2.6.6. Администрирование: простота использования.

Многокомпонентный МЭ должен обеспечивать возможность централизованного управления своими компонентами, в том числе, конфигурирования фильтров, проверки взаимной согласованности всех фильтров, анализа регистрационной информации.

Должен быть предусмотрен графический интерфейс для управления МЭ.

2.6.7. Целостность.

МЭ должен содержать средства контроля за целостностью своей программной и информационной части по контрольным суммам аттестованного алгоритма как в процессе загрузки, так и динамически.

2.6.8. Восстановление.

Данные требования полностью совпадают с аналогичными требованиями второго класса (п.2.5.8).

2.6.9. Тестирование.

В МЭ должна обеспечиваться возможность регламентного тестирования:

реализации правил фильтрации (см. п. 2.6.1);

процесса идентификации и аутентификации (см. п. 2.6.2);

процесса регистрации (см. п. 2.6.3);

процесса идентификации и аутентификации администратора МЭ (см. п. 2.6.4);

процесса регистрации действий администратора МЭ (см. п. 2.6.5);

процесса централизованного управления компонентами МЭ и графический интерфейс для управления МЭ (см. п. 2.6.6);

процесса контроля за целостностью программной и информационной части МЭ (см. п. 2.6.7);

процедуры восстановления (см. п. 2.6.8).

2.6.10. Руководство администратора МЭ.

Данные требования полностью совпадают с аналогичными требованиями пятого класса (п.2.2.7).

2.6.11. Тестовая документация.

Должна содержать описание тестов и испытаний, которым подвергался МЭ (в соответствии с п. 2.6.9), и результаты тестирования.

2.6.12. Конструкторская (проектная) документация.

Данные требования полностью включают аналогичные требования третьего класса (п. 2.4.12) по составу документации.

Дополнительно документация должна содержать описание графического интерфейса для управления МЭ.

3. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Администратор МЭ - лицо, ответственное за сопровождение МЭ.

Дистанционное управление компонентами МЭ - выполнение функций по сопровождению МЭ (компоненты) администратором МЭ с узла (рабочей станции) сети, на котором не функционирует МЭ (компонента) с использованием сетевых протоколов.

Критерии фильтрации - параметры, атрибуты, характеристики, на основе которых осуществляется разрешение или запрещение дальнейшей передачи пакета (данных) в соответствии с заданными правилами разграничения доступа (правилами фильтрации). В качестве таких параметров могут использоваться служебные поля пакетов (данных), содержащие сетевые адреса, идентификаторы, адреса интерфейсов, портов и другие значимые данные, а также внешние характеристики, например, временные, частотные характеристики, объем данных и т.п.

Локальное (местное) управление компонентами МЭ - выполнение функций по сопровождению МЭ (компоненты) администратором МЭ на том же узле (платформе), на котором функционирует МЭ (компонента) с использованием интерфейса МЭ.

Межсетевой Экран (МЭ) - это локальное (однокомпонентное) или функционально- распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в АС и/или выходящей из АС. МЭ обеспечивает защиту АС посредством фильтрации информации, т.е. ее анализа по совокупности критериев и принятия решения о ее распространении в (из) АС на основе заданных правил, проводя таким образом разграничение доступа субъектов из одной АС к объектам другой АС. Каждое правило запрещает или разрешает передачу информации определенного вида между

субъектами и объектами. Как следствие, субъекты из одной АС получают доступ только к разрешенным информационным объектам из другой АС. Интерпретация набора правил выполняется последовательностью фильтров, которые разрешают или запрещают передачу данных (пакетов) на следующий фильтр или уровень протокола.

Правила фильтрации - перечень условий, по которым с использованием заданных критериев фильтрации осуществляется разрешение или запрещение дальнейшей передачи пакетов (данных) и перечень действий, производимых МЭ по регистрации и/или осуществлению дополнительных защитных функций.

Межсетевой экран может строиться с помощью экранирующих агентов, которые обеспечивают установление соединения между субъектом и объектом, а затем пересылают информацию, осуществляя контроль и/или регистрацию. Использование экранирующих агентов позволяет предоставить дополнительную защитную функцию - сокрытие от субъекта истинного объекта. В то же время, субъекту кажется, что он непосредственно взаимодействует с объектом. Обычно экран не является симметричным, для него определены понятия «внутри» и «снаружи». При этом задача экранирования формулируется как защита внутренней области от неконтролируемой и потенциально враждебной внешней.

Сетевые адреса - адресные данные, идентифицирующие субъекты и объекты и используемые протоколом сетевого уровня модели международной организации по стандартизации взаимодействия открытых систем (ISO OSI). Сетевой протокол выполняет управление коммуникационными ресурсами, маршрутизацию пакетов, их компоновку для передачи в сети. В этих протоколах решается возможность доступа к подсети, определяется маршрут передачи и осуществляется трансляция сообщения. Управление доступом на сетевом уровне позволяет отклонять нежелательные вызовы и дает возможность различным подсетям управлять использованием ресурсов сетевого уровня. Поэтому, в данных протоколах

возможно выполнение требований по защите в части проверки подлинности сетевых ресурсов, источника и приемника данных, принимаемых сообщений, проведения контроля доступа к ресурсам сети.

Трансляция адреса - функция МЭ, скрывающая внутренние адреса объектов (субъектов) от внешних субъектов.

Транспортные адреса - адресные данные, идентифицирующие субъекты и объекты и используемые протоколом транспортного уровня модели ISO OSI. Протоколы транспортного уровня обеспечивают создание и функционирование логических каналов между программами (процессами, пользователями) в различных узлах сети, управляют потоками информации между портами, осуществляют компоновку пакетов о запросах и ответах.

Централизованное управление компонентами МЭ - выполнение с одного рабочего места (рабочей станции, узла) всех функций по сопровождению МЭ (его компонент), только со стороны санкционированного администратора, включая инициализацию, останов, восстановление, тестирование, установку и модификацию правил фильтрации данных, параметров регистрации, дополнительных защитных функций и анализ зарегистрированных событий.

Экранирование - функция МЭ, позволяющая поддерживать безопасность объектов внутренней области, игнорируя несанкционированные запросы из внешней области. В результате экранирования уменьшается уязвимость внутренних объектов, поскольку первоначально сторонний нарушитель должен преодолеть экран, где защитные механизмы сконфигурированы особенно тщательно и жестко. Кроме того, экранирующая система, в отличие от универсальной, может и должна быть устроена более простым и, следовательно, более безопасным образом, на ней должны присутствовать только те компоненты, которые необходимы для выполнения функций экранирования. Экранирование дает также возможность контролировать информационные потоки,

направленные во внешнюю область, что способствует поддержанию во внутренней области режима конфиденциальности. Помимо функций разграничения доступа, экраны осуществляют регистрацию информационных обменов