15

O‘z DSt 215:2014

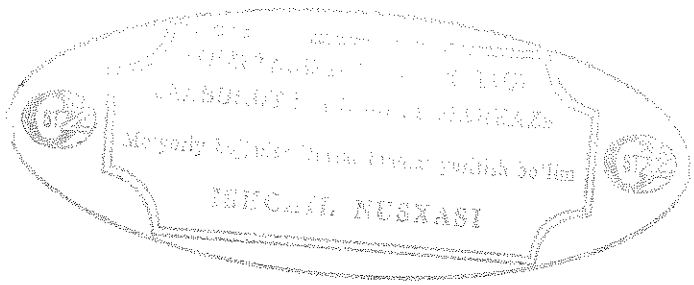
ГОСУДАРСТВЕННЫЙ СТАНДАРТ РЕСПУБЛИКИ УЗБЕКИСТАН

Информационная технология

МЕЖСЕТЕВЫЕ ЭКРАНЫ

Классификация по уровню защищенности от несанкционированного доступа к информации

Издание официальное



Узбекское агентство стандартизации, метрологии и сертификации

Ташкент

O‘z DSt 2915:2014

Предисловие

1 РАЗРАБОТАН И ВНЕСЕН Службой национальной безопасности Республики Узбекистан

2 УТВЕРЖДЕН и ВВЕДЕН В ДЕЙСТВИЕ постановлением Узбекского агентства стандартизации, метрологии и сертификации (агентство «Узстандарт») 18.03.2014 № 05-530

3 ВВЕДЕН ВПЕРВЫЕ

Информация о введении в действие (прекращении действия) настоящего стандарта и изменений к нему на территории Республики Узбекистан публикуются в указателе, издаваемом агентством «Узстандарт». В случае пересмотра или отмены настоящего стандарта соответствующая информация будет опубликована в информационном указателе, издаваемом агенством «Узстандарт».

Исключительное право официального опубликования настоящего стандарта на территории Узбекистана принадлежит агентству «Узстандарт»

STANDARTLASHTI
NAZORATINI KUCH
AXBOROT TEXN
JORIY ETISH

Содержание

1 Область применения 1
2 Нормативные ссылки 1
3 Термины и определения 2
4 Общие положения 3
5 Требования к третьему классу защищенности МЭ 5
6 Требования ко второму классу защищенности МЭ 7
7 Требования к первому классу защищенности МЭ 9

O‘ZBEKISTON RESPUBLIKASI
STANDARTLASHTIRISH, DANSAT
NAZORATINI MUVOFIQLASHTIRISH VA
AXBOROT TEXNOLOGIYALARIDA
JORIY ETISH BOSHQARMASI

ГОСУДАРСТВЕННЫЙ СТАНДАРТ РЕСПУБЛИКИ УЗБЕКИСТАН

Ахборот технологияси
ТАРМОҚЛАРАРО ЭКРАНЛАР
Ахборотдан рухсатсиз фойдалана олишдан муҳофазаланганлик даражалари буйича таснифлаш

Информационная технология
МЕЖСЕТЕВЫЕ ЭКРАНЫ
Классификация по уровню защищенности от несанкционированного доступа к информации

Information technology
Firewalls
Classification by level of protection from unauthorized access to information

Дата введения 31 03 2014

1 Область применения

Настоящий стандарт устанавливает классификацию межсетевых экранов по уровню защищенности от несанкционированного доступа к информации в соответствии с показателями защищенности и совокупностью описывающих их требований.

Стандарт предназначен для применения заказчиками и разработчиками межсетевых экранов, сетей распределенных автоматизированных систем при формулировании требований по защите от несанкционированного доступа к информации.

2 Нормативные ссылки

В настоящем стандарте использованы ссылки на следующие стандарты:

O‘z DSt ISO/IEC 2382-8:2007 Информационные технологии. Информационная безопасность. Термины и определения

O‘z DSt 1047:2003 Информационные технологии. Термины и определения

O'ZSTANDART AGENTLIGI
4/99 son bilan
« 18 » 03 2014 yilda
Davlat ro'yxatiga olindi

3 Термины и определения

В настоящем стандарте применены термины по O‘z DSt ISO/IEC 2382-8 и O‘z DSt 1047, а также следующие термины с соответствующими определениями:

3.1 **администратор МЭ**: Лицо, ответственное за сопровождение МЭ.

3.2 **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.

3.3 **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).

3.4 **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.

3.5 **межсетевой экран**; МЭ: Локальное (однокомпонентное) или функционально - распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в систему и/или выходящей из системы.

3.6 **несанкционированный доступ;** НСД**:** Доступ субъекта к объекту или информации в нарушение установленных в системе правил разграничения доступа.

3.7 **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.

3.8 **протокол**: Совокупность правил и соглашений, регламентирующих формат и процедуру передачи данных между двумя или несколькими независимыми устройствами или процессами.

3.9 **протокол транспортного уровня**: Протокол, обеспечивающий создание и функционирование логических каналов между программами (процессами, пользователями) в различных узлах сети, управляющий потоками информации между портами, осуществляющий компоновку пакетов о запросах и ответах.

3.10 **сетевой протокол**: Протокол, выполняющий управление коммуникационными ресурсами, маршрутизацию пакетов, их компоновку для передачи в сети.

3.11 **сетевые адреса**: Адресные данные, идентифицирующие субъекты и объекты и используемые протоколом сетевого уровня модели Международной организации по стандартизации взаимодействия открытых систем (ISO OSI).

3.12 **сеть ЭВМ**: Совокупность сети передачи данных, взаимосвязанных ею ЭВМ и необходимых для реализации этой связи программного обеспечения и (или) технических средств, которая предназначена для распределенной обработки информации.

3.13 **трансляция адреса**: Функция МЭ, скрывающая внутренние адреса объектов (субъектов) от внешних субъектов.

3.14 **транспортные адреса**: Адресные данные, идентифицирующие субъекты и объекты и используемые протоколом транспортного уровня модели ISO OSI.

3.15 **узел**: Компьютер в сети выполняющий основные сетевые функции (обслуживание сети, передача сообщений и т.п.).

3.16 **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, остановку, восстановление, тестирование, установку и модификацию правил фильтрации данных, параметров регистрации, дополнительных защитных функций и анализ зарегистрированных событий.

3.17 **экранирование**: Функция МЭ, позволяющая поддерживать безопасность объектов внутренней области, игнорируя несанкционированные запросы из внешней области.

4 Общие положения

4.1 МЭ обеспечивает защиту автоматизированных систем (АС) посредством фильтрации информации. На основе анализа по совокупности критериев и принятия решения о распространении информации в (из) АС, и заданных правил МЭ осуществляется разграничение доступа субъектов из одной АС к объектам другой АС. Каждое правило запрещает или разрешает передачу информации определенного вида между субъектами и объектами. 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.

4.2 МЭ строится с помощью модулей экранирования, которые обеспечивают установление соединения между субъектом и объектом, а затем пересылают информацию, осуществляя контроль и/или регистрацию. Использование экранирующих модулей предоставляет дополнительную защитную функцию - сокрытие от субъекта истинного объекта. При этом задача экранирования формулируется как защита внутренней области от неконтролируемой и потенциально враждебной внешней.

4.3 Показатели защищенности содержат требования к средствам защиты, обеспечивающим безопасное взаимодействие сетей ЭВМ, АС

O'ZBEKISTANDART AGENTLIGI
STANDARTLASHTIRISH, DAVLAT
NAZORATINI MUVOFIQLASHTIRISH VA
AXBOROT TEXNOLOGIYALARINI
JORIY ETISH BOSHQAR ASI

посредством управления межсетевыми потоками информации и реализованных в виде МЭ.

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

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

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

4.6 Устанавливается три класса защищенности МЭ.

Каждый класс характеризуется определенной минимальной совокупностью требований по защите информации в соответствии с таблицей 1.

Таблица 1 – Показатели классов защищенности МЭ

Показатель защищенности	Класс		
	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 МЭ	+	+	+
Тестовая документация	+	+	+
Конструкторская (проектная) документация	+	+	+
Предоставление отчёта	+	+	+
Примечание - «+» - есть требования к данному классу, «-» - нет требований к данному классу.			

Самый низкий класс защищенности - третий, применяемый для обеспечения безопасного взаимодействия АС, обрабатывающей конфиденциальную информацию, с внешней средой, второй - для обеспечения безопасного взаимодействия АС, обрабатывающей информацию с грифом «секретно», самый высокий - первый, применяемый для безопасного взаимодействия АС, с грифом «совершенно секретно».

5 Требования к третьему классу защищенности МЭ

5.1 Управление доступом

МЭ должен обеспечивать возможность трансляции сетевых адресов и фильтрацию на сетевом уровне:

- пакетов служебных протоколов, служащих для диагностики и управления работой сетевых устройств;
- с учетом входного и выходного сетевого интерфейса как средство проверки подлинности сетевых адресов;
- с учетом любых значимых полей сетевых пакетов.

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

5.2 Регистрация

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

5.3 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.

5.4 Администрирование: регистрация

МЭ должен обеспечивать:

- регистрацию входа (выхода) администратора МЭ в систему (из системы) либо загрузки и инициализации системы и ее программной остановки. Регистрация выхода из системы не проводится в моменты аппаратного отключения МЭ;
- регистрацию и учет фильтруемых пакетов. В параметры регистрации включаются адрес, время и результат фильтрации;
- регистрацию запуска программ и процессов (заданий, задач).

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.

5.5 Целостность

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

5.6 Восстановление

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

5.7 Тестирование

В МЭ должна обеспечиваться возможность регламентного тестирования:

- реализации правил фильтрации в соответствии с требованиями 5.1;
- процесса регистрации в соответствии с требованиями 5.2;
- процесса идентификации и аутентификации администратора МЭ в соответствии с требованиями 5.3;
- процесса регистрации действий администратора МЭ в соответствии с требованиями 5.4;
- процесса контроля за целостностью программной и информационной части МЭ в соответствии с требованиями 5.5;
- процедуры восстановления в соответствии с требованиями 5.6.

5.8 Руководство администратора МЭ

Руководство администратора МЭ должно содержать:

- описание контролируемых функций МЭ;
- руководство по настройке и конфигурированию МЭ;
- описание старта (запуска) МЭ и процедур проверки правильности старта;
- руководство по процедуре восстановления.

5.9 Тестовая документация

Тестовая документация должна содержать описание тестов и испытаний, которым подвергался МЭ в соответствии с 5.7 и результаты тестирования.

5.10 Конструкторская (проектная) документация

Конструкторская (проектная) документация должна содержать:

- общую схему МЭ;
- общее описание принципов работы МЭ;

STANDARTLASHTIRISH DAVLAT
NAZORATI ... JUVOFIQLIK SERTIFIKATI
AXBOROT TEXNOLOGIYALARI
JORIY ETISH UCHUN RUXSAT BERILDI

- 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.

5.11 Предоставление отчёта

МЭ должен иметь возможность предоставления отчёта всех регистрируемых событий при функционировании МЭ, контроля целостности и изменений, вносимых в конфигурационные файлы МЭ.

6 Требования ко второму классу защищенности МЭ

6.1 Управление доступом

Требования аналогичны требованиям третьего класса, приведенным в 5.1.

Дополнительно МЭ должен обеспечивать:

- фильтрацию на транспортном уровне запросов на установление виртуальных соединений. Учитываются транспортные адреса отправителя и получателя;
- фильтрацию на прикладном уровне запросов к прикладным сервисам. При этом учитываются прикладные адреса отправителя и получателя;
- возможность сокрытия субъектов (объектов) и/или прикладных функций защищаемой сети;
- фильтрацию с учетом даты/времени.

6.2 Идентификация и аутентификация

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

6.3 Регистрация

Требования аналогичны требованиям третьего класса, приведенным в 5.2.

Дополнительно МЭ должен обеспечивать:

- регистрацию и учет фильтруемых пакетов. В параметры регистрации включаются адрес, время и результат фильтрации;

- дистанционную сигнализацию попыток нарушения правил фильтрации;
- регистрацию и учет запрашиваемых сервисов прикладного уровня;
- программируемую реакцию на события в МЭ.

6.4 Администрирование: идентификация и аутентификация

Требования аналогичны требованиям третьего класса, приведенным в 5.3.

6.5 Администрирование: регистрация

Требования аналогичны требованиям третьего класса, приведенным в 5.4.

Дополнительно МЭ должен обеспечивать регистрацию действия администратора МЭ по изменению правил фильтрации.

6.6 Администрирование: простота использования

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

6.7 Целостность

Требования аналогичны требованиям третьего класса, приведенным в 5.5.

Дополнительно должен обеспечиваться контроль целостности программной и информационной части МЭ по контрольным суммам.

6.8 Восстановление

Требования аналогичны требованиям третьего класса, приведенным в 5.6.

6.9 Тестирование

В МЭ должна обеспечиваться возможность регламентного тестирования:

- реализации правил фильтрации в соответствии 6.1;
- процесса регистрации в соответствии 6.3;
- процесса идентификации и аутентификации запросов в соответствии 6.2;

- процесса идентификации и аутентификации администратора МЭ в соответствии 6.4;

- процесса регистрации действий администратора МЭ в соответствии 6.5;

- процесса контроля за целостностью программной и информационной части МЭ в соответствии 6.7;

- процедуры восстановления в соответствии 6.8.

6.10 Руководство администратора МЭ

Требования аналогичны требованиям третьего класса, приведенным в 5.8.

6.11 Тестовая документация

Тестовая документация должна содержать описание тестов и испытаний, которым подвергался МЭ в соответствии с 6.9 и результаты тестирования.

6.12 Конструкторская (проектная) документация

Требования по составу документации аналогичны требованиям третьего класса, приведенным в 5.10.

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

6.13 Предоставление отчёта

Требования аналогичны требованиям третьего класса, приведенным в 5.11.

7 Требования к первому классу защищенности МЭ

7.1 Управление доступом

Требования аналогичны требованиям второго класса, приведенным в 6.1.

Дополнительно МЭ должен обеспечивать возможность трансляции сетевых адресов.

7.2 Идентификация и аутентификация

Требования аналогичны требованиям второго класса, приведенным в 6.2.

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

7.3 Регистрация

Требования аналогичны требованиям второго класса, приведенным в 6.3.

7.4 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 не идентифицированного 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.

7.5 Администрирование: регистрация

Требования аналогичны требованиям второго класса, приведенным в 6.5.

7.6 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.

7.7 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.

7.8 Восстановление

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

7.9 Тестирование

В МЭ должна обеспечиваться возможность регламентного тестирования:

- реализации правил фильтрации в соответствии с требованиями 7.1;
- процесса идентификации и аутентификации в соответствии с требованиями 7.2;
- процесса регистрации в соответствии с требованиями с требованиями 7.3;
- процесса идентификации и аутентификации администратора МЭ в соответствии с требованиями с требованиями 7.4;
- процесса регистрации действий администратора МЭ в соответствии с требованиями 7.5;
- процесса контроля за целостностью программной и информационной части МЭ в соответствии с требованиями 7.7;
- процедуры восстановления в соответствии с требованиями 7.8.

7.10 Руководство администратора МЭ

Требования аналогичны требованиям третьего класса, приведенным в 5.8.

7.11 Тестовая документация

Тестовая документация должна содержать описание тестов и испытаний, которым подвергался МЭ в соответствии с 7.9 и результаты тестирования.

7.12 Конструкторская (проектная) документация

Требования по составу документации аналогичны требованиям второго класса, приведенным в 6.12.

Дополнительно документация должна содержать описание графического интерфейса для управления МЭ.

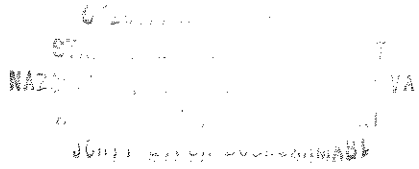
7.13 Предоставление отчёта

Требования аналогичны требованиям третьего класса, приведенным в 5.11.

O'zbekiston Agentligi
STANDARTLASHTIRISH, DAVLAT
NAZORATINI MUVOFIQLASHTIRISH VA
AXBOROT TEXNOLOGIYALARINI
JORIY ETISH BOSHQARMASI

УДК 004.056.53 ОКС 35.040 П 89

Ключевые слова: межсетевой экран, несанкционированный доступ, администрирование, защищенность, фильтрация



Сотрудник Службы
национальной безопасности
Республики Узбекистан — Д. Мажидов
12.03.2014г.

Нормоконтроль — Л. Шаймарданова
12.03.2014

СОГЛАСОВАНО

Государственный комитет
связи, информатизации и
телекоммуникационных
технологий Республики
Узбекистан

письмо от 26.02.2014
№ 14-8/1125