Описание функциональных характеристик

ОС «Циркон 37К»

СОДЕРЖАНИЕ

1. Общие сведения

ОС «Циркон 37К» сертифицировано в Системе сертификации средств защиты информации по требованиям безопасности информации № РОСС RU.0001.01БИ00 и имеет сертификат соответствия № 4444 (выдан ФСТЭК России 23.09.2021 г., действителен до 23.09.2026 г.).

Согласно сертификату, ОС «Циркон 37К» соответствует требованиям по безопасности информации, установленным в документах:

- «Требования безопасности информации к операционным системам» (утверждены приказом ФСТЭК России от 19 августа 2016 г. № 119);
- Методический документ ФСТЭК России «Профиль защиты операционных систем типа «А» четвертого класса защиты. ИТ.ОС.А4.ПЗ. (утвержден ФСТЭК России 8 февраля 2017 г.);
- «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий» (утверждены приказом ФСТЭК России от 02 июня 2020 г. № 76) ‧ по 4 уровню доверия;
- «Операционная система «Циркон 37К». Задание по безопасности. СДЕМ.00080-01 99 01».

при выполнении указаний по эксплуатации, приведенных в формуляре.

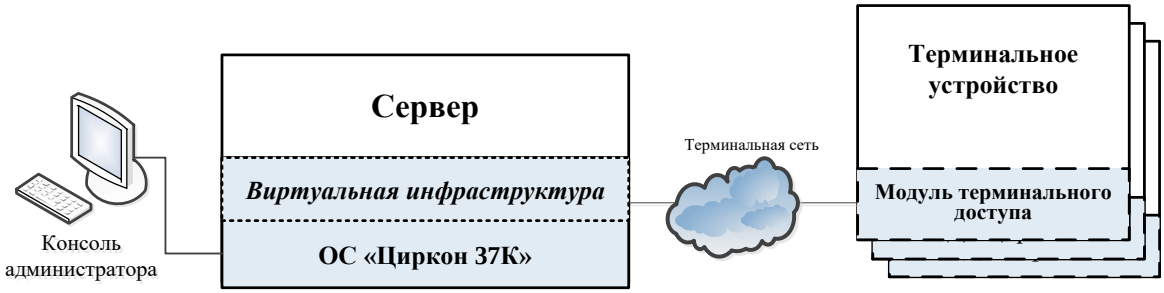
ОС «Циркон 37К» может использоваться для создания:

- значимых объектов критической информационной инфраструктуры 1 категории в соответствии с документом «Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации», утвержденные приказом ФСТЭК России от 25 декабря 2017 г. № 239 и со статьей 7 Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации;

- государственных информационных систем до 1 класса защищенности включительно в соответствии с документом «Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», утвержденным приказом ФСТЭК России от 11 февраля 2013 г. № 17 с изменениями, внесенными приказом ФСТЭК России от 15.02.2017 №27»;
- информационных систем персональных данных до 1 уровня защищенности включительно в соответствии с документом «Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденным приказом ФСТЭК России от 18 февраля 2013 г. № 21 с изменениями, внесенными приказом ФСТЭК России от 23.03.2017 № 49»;
- информационных систем общего пользования 2 класса.

2. Назначение и область применения ОС «Циркон 37К»

Операционная система «Циркон 37К» (далее – ОС «Циркон 37К») представляет собой операционную систему общего пользования со встроенным гипервизором и программным модулем терминального доступа ОС «Циркон 37К» (далее – МТД ОС «Циркон 37К»). Она может использоваться для построения виртуальной инфраструктуры с подключением терминальных устройств.



ОС «Циркон 37К» предназначена для защиты от несанкционированного доступа к информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну, хранимой и обрабатываемой на серверах, включая доступ к виртуальной инфраструктуре, разворачиваемой на основе использования встроенного гипервизора ОС «Циркон 37К».

За счет наличия в составе ОС «Циркон 37К» гипервизора, появляется возможность одновременного выполнения нескольких операционных систем посредством виртуализации и управления устройствами, вычислительными процессами, а также эффективного распределения вычислительных ресурсов между виртуальными машинами.

ОС «Циркон 37К» разработана на базе ОС Debian 10.

ОС «Циркон 37К» предназначена для установки на серверах архитектуры x86-64. Для доступа пользователей к виртуальной инфраструктуре через терминальные устройства используется МТД ОС «Циркон 37К».

МТД ОС «Циркон 37К» состоит из серверной части, функционирующей под управлением ОС «Циркон 37К» и терминальной части, функционирующей на терминальном устройстве.

МТД ОС «Циркон 37К» включает:

- загрузчик U-boot (далее – начальный загрузчик МТД ОС «Циркон 37К»);
- ядро с файловой системой RootFS и терминальным клиентом, обеспечивающим взаимодействие с сервером по протоколам SSH и TigerVNC (далее – ядро МТД ОС «Циркон 37К»).

Ядро МТД ОС «Циркон 37К» хранится в служебном виртуальном домене, а также может быть записано в энергонезависимую память терминального устройства. Оно загружается в оперативную память терминального устройства и получает управление только после проверки целостности начальным загрузчиком МТД ОС «Циркон 37К».

Серверная часть МТД ОС «Циркон 37К» реализует разграничение доступа пользователей к ресурсам разной степени конфиденциальности путем предоставления им возможности безопасной работы только с ресурсами выбранного пользовательского домена, а также терминальной части, функционирующей на терминальном устройстве.

Данное свойство реализуется за счет того, что:

- терминальное устройство имеет энергонезависимую память, защищенную от перезаписи, в которую на начальном этапе была записана программа-загрузчик (U-boot), которая с помощью протоколов DHCP и HTTP умеет находить в сети, скачивать и проверять на подлинность PXE-образ. После скачивания и проверки управление передается на PXE-образ, который и будет работать до выключения терминального устройства;
- переключение между разными пользовательскими доменами происходит через выключение питания на терминале (происходящее при извлечении смарт-карты), таким образом, никакой остаточной информации на терминальном устройстве не остается;

- автоматический выбор домена осуществляется за счет соответствующей записи на пользовательской смарт-карте, т.е. у пользователя должно быть столько смарт-карт, сколько существует доменов, к которым он должен (может) иметь доступ.

Используемые смарт-карты: ACOS-16, ACOS-32 и ACOS-72.

Двухфакторная аутентификация пользователя на сервере проводится за счет введения логина и пароля, а также проверки по открытому и закрытому ключу (открытый ключ пользователя хранится на сервере, а закрытый записан на смарт-карту и автоматически считывается в момент аутентификации пользователя).

Данные меры, учитывая изолированную программную среду пользователя на терминале и обязательную аутентификацию пользователя на сервере, позволяют отказаться от необходимости применения аппаратно-программных модулей доверенной загрузки на терминальных устройствах.

В качестве терминального устройства используется специализированный компьютер ARM-архитектуры с низким уровнем энергопотребления, позволяющий подключать один или два монитора, клавиатуру со смарт-карт ридером (или с отдельным смарт-карт ридером), подключаемый по витой паре к сети Ethernet (возможно оптоволоконное подключение). Дополнительно в состав терминального устройства могут входить: колонки (наушники), принтер, привод оптических дисков, USB-флеш-накопители.

3. Функциональные характеристики

В ОС «Циркон 37К» реализованы следующие функции безопасности:

- идентификация и аутентификация;
- управление доступом;
- регистрация событий безопасности;
- ограничение программной среды;
- изоляция процессов;
- защита памяти;
- контроль целостности;
- обеспечение надежного функционирования;
- фильтрация сетевого потока;
- защита виртуальной инфраструктуры.

ОС «Циркон 37К» обеспечивает следующие функциональные возможности:

1) возможность задания политики дискреционного и ролевого управления доступом для установленного множества операций, выполняемых субъектами доступа по отношению к объектам доступа;

2) возможность реализации дискреционного и ролевого управления доступом на основе списков управления доступом (или матрицы управления доступом) и (или) ролей;

3) возможность осуществления резервного копирования объектов файловой системы;

4) возможность удаления объектов файловой системы;

5) возможность восстановления объектов ОС из резервных копий, созданных с использованием ОС, и использования ассоциированных с ними атрибутов безопасности;

6) возможность установки ПО (компонентов ПО) только администраторами;

7) возможность задания правил автоматического запуска компонентов ПО при загрузке ОС;

8) контроль запуска компонентов ПО и реагирование на попытки запуска компонентов ПО, произведенные в нарушение установленных правил запуска компонентов ПО;

9) возможность осуществлять фильтрацию входящих и (или) исходящих сетевых потоков;

10) возможность осуществлять фильтрацию сетевых потоков, основанную на следующих типах атрибутов безопасности субъектов доступа: сетевой адрес узла отправителя; сетевой адрес узла получателя; и информации: сетевой протокол, который используется для взаимодействия;

11) возможность явно разрешать сетевой поток, базируясь на устанавливаемом администратором наборе правил фильтрации сетевого трафика, основанном на идентифицированных атрибутах;

12) возможность запрещать сетевой поток, базируясь на устанавливаемом администратором наборе правил фильтрации сетевого трафика, основанном на идентифицированных атрибутах;

13) возможность удаления объектов файловой системы путем многократной перезаписи уничтожаемых (стираемых) объектов файловой системы специальными битовыми последовательностями;

14) обеспечение недоступности остаточной информации при распределении или освобождении ресурса памяти;

15) возможность задания правил запуска компонентов ПО в процессе функционирования ОС;

16) контроль целостности компонентов ПО, разрешенного для запуска, и реагирование на попытки запуска компонентов ПО, целостность которых была нарушена;

17) возможность осуществлять фильтрацию сетевого потока, основанную на атрибутах: разрешенные (запрещенные) протоколы прикладного уровня;

18) возможность осуществлять фильтрацию сетевого потока, основанную на следующих типах атрибутов безопасности информации: транспортный протокол, который используется для взаимодействия, порты источника и получателя в рамках сеанса (сессии);

19) возможность поддерживать для каждого пользователя ОС список атрибутов безопасности;

20) возможность блокирования учетной записи пользователя ОС при превышении установленного администратором числа неуспешных попыток аутентификации;

21) обеспечение идентификации объектов доступа;

22) идентификация пользователя до выполнения действий по доступу в информационную систему или администратора до выполнения действий по управлению ОС;

23) исключение отображения действительного значения аутентификационной информации при ее вводе пользователем ОС в диалоговом интерфейсе;

24) возможность ассоциировать атрибуты безопасности пользователя ОС с субъектами доступа (запускаемыми от его имени процессами);

25) возможность проверки соответствия аутентификационной информации метрике качества, обеспечивающей адекватную защиту от нарушения безопасности нарушителем с потенциалом нападения, соответствующим классу защищенности;

26) идентификация и аутентификация пользователя до выполнения любых действий по доступу в информационную систему или администратора до выполнения действий по управлению ОС;

27) возможность поддержки многофакторной или двухфакторной аутентификации;

28) возможность со стороны администратора управлять атрибутами безопасности;

29) возможность со стороны администратора управлять выполнением функций безопасности ОС;

30) возможность со стороны администратора управлять параметрами функций безопасности ОС, данными аудита, правилами фильтрации сетевого потока;

31) поддержка определенных ролей для ОС и их ассоциации с пользователями ОС;

32) возможность применения наборов базовых конфигураций ОС;

33) возможность устанавливать пороговое значение количества неуспешных попыток аутентификации, предоставляемая администратору;

34) возможность устанавливать срок действия паролей, предоставляемая администратору;

35) возможность устанавливать срок действия идентификаторов для временных учетных записей, предоставляемая администратору;

36) обеспечение ограничительных значений по умолчанию для атрибутов безопасности, которые используются для осуществления политики дискреционного управления доступом;

37) обеспечение управления доступом к объектам ОС;

38) защита хранимой аутентификационной информации от неправомерного доступа к ней и раскрытия;

39) обеспечение защиты от переполнения буфера;

40) постоянный контроль и проверка правомочности обращений субъектов доступа к объектам доступа;

41) возможность предоставления надежных меток времени при проведении аудита, а также для ограничения срока действий атрибутов безопасности;

42) возможность тестирования (самотестирования) функций безопасности ОС, проверки целостности ПО ОС и целостности данных (параметров) ОС;

43) возможность возврата ОС при сбоях и отказах к безопасному состоянию в автоматизированном режиме;

44) возможность работы экземпляров ОС на нескольких технических средствах в отказоустойчивом режиме, обеспечивающем доступность сервисов и информации при выходе из строя одного из технических средств (отказоустойчивый кластер);

45) возможность работы экземпляров ОС на нескольких технических средствах в режиме балансировки нагрузки, обеспечивающем доступность сервисов и информации в условиях компьютерных атак, направленных на отказ в обслуживании, приводящих к полному исчерпанию вычислительных ресурсов одного из технических средств (кластер с балансировкой нагрузки);

46) возможность предоставления приоритетов для использования субъектами доступа подмножества вычислительных ресурсов средства вычислительной техники под контролем функций безопасности ОС;

47) возможность квотирования ОС вычислительных ресурсов средства вычислительной техники;

48) возможность осуществлять блокирование сеанса доступа пользователя ОС по истечении заданного интервала времени бездействия;

49) возможность осуществлять блокирование (разблокирование) собственного сеанса доступа в ОС пользователем ОС;

50) возможность автоматически осуществлять блокирование интерактивного сеанса пользователя ОС после установленного периода бездействия;

51) возможность осуществлять блокирование интерактивного сеанса по требованию уполномоченного привилегированного субъекта доступа;

52) возможность в ОС отдельно осуществлять ограничение максимального числа одновременных (параллельных) интерактивных сеансов, предоставляемых уполномоченным привилегированным субъектам доступа и уполномоченным непривилегированным субъектам доступа;

53) возможность обеспечения защиты от несогласованностей, возникающих на уровне процессов при параллельной работе с ресурсами средства вычислительной техники и объектами доступа ОС;

54) возможность блокирования попыток доступа к объектам доступа, если в момент обращения они используются другими процессами;

55) возможность безопасного выделения областей оперативной памяти;

56) возможность регистрации и учета выполнения проверок при фильтрации сетевого потока;

57) возможность реагирования при обнаружении событий, указывающих на возможное нарушение безопасности;

58) возможность включения и исключения событий в совокупность событий, подвергающихся аудиту, предоставляемая администратору;

59) возможность предоставления администратору всей информации аудита в понятном для него виде;

60) возможность защиты хранимых записей регистрации событий безопасности ОС (аудита) от несанкционированного удаления и предотвращения модификации записей аудита;

61) возможность выполнения действий, направленных на сохранение данных журнала регистрации событий безопасности ОС и обеспечивающих непрерывность процесса аудита, если журнал регистрации событий безопасности ОС превысит определенный администратором размер;

62) возможность регистрации (аудита) событий безопасности, которые в соответствии с национальным стандартом Российской Федерации ГОСТ Р ИСО/МЭК 15408-2-2013 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные компоненты безопасности» включены в базовый уровень аудита;

63) возможность просмотра записей аудита только администратором;

64) возможность выборочного просмотра данных регистрации (аудита) событий безопасности ОС (поиск, сортировка, упорядочение данных аудита);

65) возможность выполнения действий, направленные на предотвращение потери данных аудита при переполнении журнала регистрации событий безопасности ОС;

66) возможность полнотекстовой регистрации привилегированных команд (команд, управляющих системными функциями);

67) возможность передавать данные аудита для внешнего хранения.

4. Входные и выходные данные

Входными данными ОС являются:

- действия пользователя в графическом интерфейсе (нажатие кнопок, заполнение полей, выбор пунктов в списках и т.д.);
- команды, вводимые пользователем в консоли;
- системные конфигурационные файлы;
- информация, получаемая по сетевым интерфейсам.

Выходными данными ОС являются:

- данные, отображаемые средствами графического интерфейса;
- результаты выполнения команд пользователя, выводимые в консоль;
- файлы и документы в различных форматах, созданные при помощи текстовых, табличных, графических и иных редакторов;
- записи в системных журналах;
- информация, отправляемая по сетевым интерфейсам.

АКЦИОНЕРНОЕ ОБЩЕСТВО
"МНОГОПРОФИЛЬНОЕ
ВНЕДРЕНЧЕСКОЕ ПРЕДПРИЯТИЕ
"СВЕМЕЛ"

127254, г. Москва, Огородный пр., д. 5, стр.5
Тел/Факс: +7(495) 926-7187, +7(499) 750-7065
E-mail: post@swemel.ru