УТВЕРЖДЕН
ПФНА.501410.001 31-ЛУ

СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ В ВИРТУАЛЬНЫХ ИНФРАСТРУКТУРАХ «Dallas Lock»

Описание применения

ПФНА.501410.001 31

Листов 14

Аннотация

Данный документ выполнен в соответствии с ГОСТ 19.502-78 и распространяется на изделие «Система защиты информации в виртуальных инфраструктурах «Dallas Lock» ПФНА.501410.001 31 (далее по тексту – «изделие» или СЗИ ВИ Dallas Lock).

В настоящем документе содержатся общие сведения о назначении изделия и программного обеспечения изделия (далее по тексту – «ПО изделия» или «СЗИ ВИ»), условиях применения, описание задачи, перечень входных и выходных данных.

Содержание

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

VMware vSphere	платформа (среда) виртуализации серверов/рабочих станций с возможностями согласованного управления виртуальными ЦОД (центр обработки данных)
VMware vCenter Server (сервер виртуализации)	платформа для централизованного управления средами VMware vSphere, которая обеспечивает автоматизацию и надежное предоставление виртуальной инфраструктуры
vSphere Hypervisor ESXi (Гипервизор ESXi)	программа или аппаратная схема, обеспечивающая или позволяющая одновременное, параллельное выполнение нескольких или даже многих операционных систем на одном и том же хост-компьютере
AD (Active Directory)	LDAP-совместимая реализация службы каталогов корпорации Microsoft для операционных систем семейства Windows Server
ТС	техническое средство
ВИ	виртуальная инфраструктура Dallas Lock
ВМ	виртуальная машина
ОС	операционная система
Dallas Lock 8.0	компонент СЗИ ВИ на базе Dallas Lock 8.0-К или Dallas Lock 8.0-С
СБ	компонент СЗИ ВИ на базе сервера безопасности Dallas Lock 8.0-К или сервера безопасности Dallas Lock 8.0-С

1. НАЗНАЧЕНИЕ

1.1. СЗИ ВИ Dallas Lock предназначена для защиты среды виртуализации на базе VMware vSphere (гипервизор ESXi 5.5[1] и 6.0) от несанкционированного доступа при работе в многопользовательских автоматизированных системах (АС), государственных информационных системах (ГИС), в автоматизированных системах управления (АСУ), информационных системах персональных данных (ИСПДн).

1.2. Изделие предназначено для использования на персональных компьютерах и узлах виртуальной инфраструктуры в составе локальной вычислительной сети.

[1] Для защиты среды виртуализации на базе гипервизора ESXi 5.5 необходимо применять сертифицированную версию изделия СЗИ ВИ Dallas Lock 376.3.

2. УСЛОВИЯ ПРИМЕНЕНИЯ

2.1. Изделие СЗИ ВИ Dallas Lock основано на базе СЗИ НСД Dallas Lock 8.0 и Сервера безопасности Dallas Lock 8.0 с сохранением функциональности и включает в себя следующие компоненты:

- ядро системы защиты информации в виртуальных инфраструктурах (далее по тексту Ядро СЗИ ВИ);
- компонент на базе Dallas Lock 8.0 (далее по тексту Dallas Lock 8.0);
- компонент на базе Сервера Безопасности Dallas Lock 8.0 (далее по тексту СБ);
- агент DL ESXi для гипервизора ESXi;
- агент DL vCenter для сервера виртуализации vCenter.

Программная часть Ядра СЗИ ВИ представляет из себя программную надстройку над СБ для возможности работы с объектами ВИ (Далее по тексту СБ ВИ).

2.2. Изделие предназначено для защиты виртуальной инфраструктуры с программным и техническим обеспечением, состав и характеристики которого приведены ниже.

ТС с установленным VMware vCenter Server 6.0 должна иметь следующий состав и характеристики программно-технического обеспечения.

1) Поддерживаемые ОС:

- Windows Server 2008 (SP 2) 64-bit (Standard, Enterprise, Datacenter, Web Server 2008, Storage Server 2008);
- Windows Server 2008 R2 64-bit (Standard, Enterprise, Datacenter, Web Server 2008, Storage Server 2008);
- Windows Server 2008 R2 (SP 1) 64-bit (Foundation, Standard, Web, Enterprise, Datacenter);
- Windows Server 2012 64-bit (Foundation, Essentials, Standard, Datacenter);
- Windows Server 2012 R2 64-bit (Foundation, Essentials, Standard, Datacenter).

2) Минимальная конфигурация ТС:

- процессор: Intel или AMD с 2-мя логическими ядрами по 2 ГГц каждое;
- ОЗУ – минимум 12 Гб;
- ПЗУ – минимум 60 Гб;

– сетевая карта.

Аппаратная конфигурация ТС для СБ ВИ определяется системными требованиями установленной ОС (с сетевой картой). Поддерживаются следующие версии ОС:

– Windows Server 2008 (SP 2) (Standard, Enterprise, Datacenter, Web Server 2008, Storage Server 2008);
– Windows 7 (SP 1) (Ultimate, Enterprise, Professional, Home Premium, Home Basic, Starter);
– Windows Server 2008 R2 (Foundation, Standard, Web, Enterprise, Datacenter);
– Windows Server 2008 R2 (SP 1) (Foundation, Standard, Web, Enterprise, Datacenter);
– Windows 8 (Core, Pro, Enterprise);
– Windows Server 2012 (Foundation, Essentials, Standard, Datacenter);
– Windows 8.1 (Core, Pro, Enterprise);
– Windows Server 2012 R2 (Foundation, Essentials, Standard, Datacenter);
– Windows 10 (Enterprise, Education, Pro, Home);
– Windows Server 2016 (Multipoint Premium Server, Essentials, Standard, Datacenter, Storage Server, Hyper-V Server).

ТС с установленным гипервизором VMWare ESXi 6.0 должна иметь следующий состав и характеристики программно-технического обеспечения:

– процессор: Intel или AMD с 2-мя логическими ядрами по 2 ГГц каждое, только x64;
– ОЗУ – минимум 8 Гб;
– ПЗУ – минимум 60 Гб;
– сетевая карта.

2.3. Средства управления виртуальной инфраструктурой могут быть использованы как в сетях с доменной организацией, так и в одноранговых сетях.

2.4. Изделие может быть использовано в многопользовательских автоматизированных системах (АС) и информационных системах персональных данных (ИСПДн), государственных информационных системах (ГИС), автоматизированных системах управления производственными и технологическими процессами (АСУ ТП).

2.5. Для модулей изделия СЗИ ВИ Dallas Lock предусмотрен механизм проверки наличия более новых версий.

2.6. СЗИ ВИ Dallas Lock соответствует требованиям руководящих и методических документов (требования безопасности информации ФСТЭК России):

- «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» (Гостехкомиссия России, 1992) – по 5 классу защищенности;
- «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей» (Гостехкомиссия России, 1999) – по 4 уровню контроля.

2.7. При условии соблюдения ограничений, указанных в разделе 3 формуляра на данное изделие (ПФНА.501410.001 ФО), СЗИ ВИ Dallas Lock может быть использована:

- при создании защищенных автоматизированных систем до класса защищенности 1Г включительно (Руководящий документ «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» (Гостехкомиссия России, 1992));
- для обеспечения 1 уровня защищенности персональных данных (Приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»);
- в государственных информационных системах 1 класса защищённости (Приказ ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»);
- при создании защищенных информационных систем 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 до 1 класса защищенности включительно (Приказ ФСТЭК России от 14 марта 2014 г. № 31 «Об утверждении Требований 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»).

3. ОПИСАНИЕ ЗАДАЧИ

3.1. Изделие разработано в соответствии с требованиями, описанными в документе «Технические условия» ПФНА.501410.001 ТУ (ТУ).

3.2. В соответствии с ТУ СЗИ ВИ Dallas Lock состоит из программного ядра и следующих подсистем:

- подсистема управления пользователями;
- подсистема управления доступом к объектам виртуальной инфраструктуры, к файлам и каталогам;
- подсистема гарантированной очистки памяти;
- подсистема контроля целостности;
- подсистема контроля печати;
- подсистема аудита.

3.3. Подсистема управления пользователями

3.3.1. Реализована идентификация и аутентификация администраторов и пользователей в виртуальной среде по идентификатору (коду) и паролю условно-постоянного действия – на СБ ВИ и сервере виртуализации vCenter. Контроль пользователей, имеющих право на вход на гипервизор ESXi должен осуществляться посредством выполнения необходимых настроек на стороне СБ ВИ и процесса синхронизации гипервизора с СБ ВИ.

3.3.2. Обеспечивает запрет доступа к защищаемым ресурсам неидентифицированных пользователей и пользователей, подлинность идентификации которых при аутентификации не подтвердилась. Контроль пользователей, имеющих право на доступ к гипервизору ESXi при условии успешной авторизации должен осуществляться посредством выполнения необходимых настроек на стороне СБ ВИ и процесса синхронизации гипервизора ESXi с СБ ВИ.

3.3.3. Реализовано управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов. В качестве идентификатора может выступать:

- имя локального пользователя ОС сервера виртуализации vCenter;
- имя доменного пользователя AD при условии, что СБ ВИ, сервер виртуализации vCenter, введены под управление AD и на сервере виртуализации vCenter подключен контроллер домена в качестве возможного средства проверки авторизации. Вход доменных пользователей возможен только на СБ ВИ и сервере виртуализации vCenter;
- имя пользователя из встроенной системы авторизации, входящей в состав Single Sign-On (пользователи vsphere.local*);
- имя пользователя ОС на гипервизоре ESXi.

3.3.4. Реализовано управление средствами аутентификации, в том числе хранение, выдача и инициализация всех компонент защищаемой виртуальной инфраструктуры. Осуществляется блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации для сервера виртуализации и СБ ВИ.

3.3.5. Для СБ ВИ реализована защита обратной связи при вводе аутентификационной информации, посредством замены вводимых знаков на специальные символы, не позволяющие однозначно определить вводимые знаки.

3.3.6. Реализована возможность разделения полномочий (ролей, типов учётных записей) пользователей, администраторов и лиц, обеспечивающих функционирование СЗИ ВИ Dallas Lock.

3.3.7. В программном обеспечении изделия реализовано ограничение неуспешных попыток авторизации в компонентах защищенной виртуальной инфраструктуры: гипервизорах ESXi, СБ ВИ, серверах виртуализации vCenter.

3.3.8. Для СБ ВИ и сервера виртуализации vCenter реализовано ограничение числа параллельных сеансов доступа для каждой учётной записи пользователя. Исключение составляют локальные пользователи гипервизора ESXi и пользователи, входящие в состав Single Sign-On (пользователи vsphere.local*).

3.4. Подсистема управления доступом

3.4.1. Подсистема контроля доступа к объектам виртуальной инфраструктуры

3.4.1.1. Реализовано разграничение доступа к следующим компонентам виртуальной инфраструктуры – к СБ ВИ и серверу виртуализации vCenter. Разграничение доступа к гипервизорам ESXi и виртуальным машинам ESXi (файлам виртуальных машин) реализуется в пределах ролевой модели разграничения доступа vSphere 6.0.

3.4.1.2. Осуществляется контроль доступа к операциям, выполняемым с помощью средств управления виртуальными машинами, в том числе к операциям создания, запуска, остановки, создания копий, удаления виртуальных машин, которые должны быть разрешены только назначенным пользователям.

3.4.2. Подсистема разграничения доступа к файлам и каталогам

3.4.2.1. Реализовано разграничение доступа по дискреционному принципу к объектам файловой системы и устройствам в виртуальной среде – на СБ ВИ и сервере виртуализации vCenter. Разграничение доступа к гипервизорам ESXi и виртуальным машинам (файлам виртуальных машин) реализуется в пределах ролевой модели разграничения доступа vSphere 6.0.

3.4.2.2. Для каждой пары (субъект – объект) в СЗИ ВИ Dallas Lock задано явное и недвусмысленное перечисление допустимых типов доступа т.е. тех типов доступа, которые являются санкционированными для данного

субъекта (индивида или группы индивидов) к данному ресурсу информационной системы (объекту) или среды управления виртуализацией.

3.4.2.3. Механизм, реализующий дискреционный принцип контроля доступа, предусматривает возможности санкционированного изменения правил разграничения доступа, в том числе возможность санкционированного изменения списка пользователей информационной системы и списка защищаемых объектов.

3.4.2.4. Предусмотрены средства управления, ограничивающие распространение прав на доступ.

3.5. Подсистема гарантированной очистки памяти

3.5.1. При первоначальном назначении или при перераспределении внешней памяти СЗИ ВИ Dallas Lock предотвращает доступ субъекту к остаточной информации. Осуществляется очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ, освобождаемых областей памяти внешних накопителей. Очистка осуществляется однократной произвольной записью в освобождаемую область памяти, ранее использованную для хранения защищаемых данных (файлов). На гипервизоре ESXi осуществляется очистка остаточной информации по отношению к процессу удаления виртуальных машин и, соответственно, обеспечения невозможности восстановления информации, которую данные виртуальные машины содержали до удаления.

3.6. Подсистема контроля целостности

3.6.1. Осуществляется контроль целостности компонентов виртуальной среды – на СБ ВИ и сервере виртуализации vCenter (периодический, по расписанию, по запросу), на гипервизоре ESXi (периодический, по запросу), на ВМ (периодически). По отношению к гипервизору ESXi контроль целостности возможен к следующим защищаемым видам ресурсов:

- системные файлы;
- образы дисков виртуальных машин (файлы *.vmdk);
- конфигурационные файлы виртуальных машин (виртуальное оборудование, настройки BIOS и пр.).

3.7. Подсистема контроля печати

3.7.1. Для СБ ВИ и сервера виртуализации vCenter осуществляется контроль за переносом информации на твёрдую копию посредством контроля доступа к принтерам.

3.8. Подсистема аудита

3.8.1. Осуществляется регистрация входа (выхода) субъектов доступа в систему (из системы), либо регистрация загрузки и инициализации операционной системы и ее программного останова (для СБ ВИ и сервера виртуализации vCenter). Регистрация выхода из системы или останова не проводится в моменты аппаратурного отключения АС. В параметрах регистрации указываются:

- дата и время входа (выхода) субъекта доступа в систему (из системы) или загрузки (останова) системы;
- результат попытки входа: успешная или неуспешная - несанкционированная;
- идентификатор (код или фамилия) субъекта, предъявленный при попытке доступа;
- код или пароль, предъявленный при неуспешной попытке (исключение пользователи входящие в состав Single Sign-On (пользователи vsphere.local*)).

Для гипервизоров ESXi регистрация осуществляется в пределах имеющейся информации в журналах сервера виртуализации и собственных журналах гипервизора, анализируемых и собираемых СБ ВИ.

3.8.2. Для СБ ВИ и сервера виртуализации осуществляется регистрация выдачи печатных (графических) документов на «твёрдую» копию. В параметрах регистрации указываются:

- дата и время выдачи (обращения к подсистеме вывода);
- спецификация устройства выдачи [логическое имя (номер) внешнего устройства];
- наименование и уровень конфиденциальности документа (общедоступная информация);
- идентификатор субъекта доступа, запросившего документ.

3.8.3. Для всех компонентов виртуальной инфраструктуры с ОС семейства Windows (включая сервер виртуализации vCenter) осуществляется регистрация запуска (завершения) программ и процессов (заданий, задач), предназначенных для обработки защищаемых файлов. В параметрах регистрации указываются:

- дата и время запуска;
- имя (идентификатор) программы (процесса, задания);
- идентификатор субъекта доступа, запросившего программу (процесс, задание);
- результат запуска (успешный, неуспешный - несанкционированный).

3.8.4. Для сервера виртуализации vCenter и гипервизоров ESXi, в пределах имеющейся информации в журналах сервера виртуализации vCenter, осуществляется регистрация попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам. В параметрах регистрации указываются:

- дата и время попытки доступа к защищаемому файлу с указанием ее результата: успешная, неуспешная - несанкционированная;

– идентификатор субъекта доступа;
– спецификация защищаемого файла.

3.8.5. Для сервера виртуализации vCenter и гипервизоров ESXi, в пределах имеющейся информации в журналах сервера виртуализации vCenter, осуществляется регистрация следующих событий:

– запуск, остановка и конфигурирование ВМ;
– запуск (завершение) работы компонентов виртуальной инфраструктуры;
– доступ субъектов доступа к компонентам виртуальной инфраструктуры;
– изменения в составе и конфигурации компонентов виртуальной инфраструктуры во время их запуска, функционирования и аппаратного отключения.

Для каждого события регистрируется следующая информация:

– дата и время;
– субъект, осуществляющий регистрируемое действие;
– тип события (если регистрируется запрос на доступ, то следует отмечать объект и тип доступа);
– успешно ли осуществилось событие (обслужен запрос на доступ или нет).

3.8.6. Реализована возможность определения типов событий безопасности, подлежащих регистрации, для всех компонентов виртуальной инфраструктуры с ОС семейства Windows (за исключением серверов виртуализации).

3.8.7. Для СБ ВИ реализована возможность определения состава и содержания информации о событиях безопасности, подлежащих регистрации.

3.8.8. СЗИ ВИ Dallas Lock содержит средства выборочного ознакомления с регистрационной информацией.

3.8.9. В СЗИ ВИ Dallas Lock реализована возможность просмотра и анализа информации о действиях отдельных пользователей в информационной системе (в т. ч. среде виртуализации и на ВМ).

3.9. Доработка существующих подсистем

3.9.1. СЗИ ВИ Dallas Lock блокирует подключения к серверу виртуализации vCenter с несанкционированных удаленных консолей.

4. ВХОДНЫЕ И ВЫХОДНЫЕ ДАННЫЕ

4.1. Входные данные

Входными данными являются:

- дерево объектов для каждой из развернутых и защищаемых виртуальных инфраструктур;
- список субъектов доступа, идентифицируемых логином (локальные пользователи Windows, доменные пользователи Windows, локальные пользователи гипервизоров, пользователи домена vsphere.local (Single Sign-On);
- настроенный набор ролей, определяющих полномочия по использованию объектов виртуальной инфраструктуры и их администрированию;
- список служб гипервизоров.

4.2. Выходные данные

Выходными данными являются:

- Журнал событий, создаваемый сервером виртуализации в процессе работы, и журналы гипервизоров, анализируемые и собираемые СБ ВИ, собственный журнал событий безопасности СБ ВИ;
- значения контрольных сумм объектов, на которых установлен контроль целостности;
- файлы конфигураций модулей СЗИ ВИ Dallas Lock.
- сообщения СЗИ ВИ Dallas Lock в случае сигнализации при попытках несанкционированного доступа.

В журналах событий отслеживаются и отображаются такие данные, как дата, время, имя пользователя, имя объекта виртуальной инфраструктуры, тип события, результат, характер ошибки, фиксируются действия служб гипервизоров и иная информация.