УТВЕРЖДЕН
ПФНА.501410.001 31-ЛУ

СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ В ВИРТУАЛЬНЫХ ИНФРАСТРУКТУРАХ «Dallas Lock»

Описание применения

ПФНА.501410.001 31

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, условиях применения, описание задачи, перечень входных и выходных данных.

Содержание

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ 4

1. НАЗНАЧЕНИЕ 6

2. УСЛОВИЯ ПРИМЕНЕНИЯ 7

3. ОПИСАНИЕ ЗАДАЧИ 11

4. ВХОДНЫЕ И ВЫХОДНЫЕ ДАННЫЕ 18

4.1. Входные данные 18

4.2. Выходные данные 18

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

ESXi	гипервизор ESXi. Средство виртуализации VMware vSphere
Hyper-V	гипервизор Hyper-V. Средство виртуализации Microsoft Hyper-V
Microsoft Hyper-V	платформа (среда) виртуализации серверов/рабочих станций 64x ОС Windows
vCenter	VMware vCenter Server. Сервер централизованного управления средством виртуализации ESXi (vCenter for Windows)
vCSA	VMware vCenter Server Appliance. Сервер управления средством виртуализации ESXi (vCenter на виртуальной машине на базе ОС Photon)
VMware vSphere	платформа (среда) виртуализации серверов/рабочих станций с возможностями согласованного управления виртуальными центрами обработки данных
Агент DL ESXi	компонент защиты гипервизора ESXi
Агент DL Hyper-V	компонент защиты гипервизора Hyper-V
Агент DL vCenter for Windows	компонент защиты сервера vCenter for Windows
Агент DL vCSA	компонент защиты сервера vCSA
АУД	агент управления доступом. Компонент Центра управления СЗИ ВИ Dallas Lock, устанавливаемый также на объекты ВИ – сервер vCenter for Windows и гипервизор Hyper-V
ВИ	виртуальная инфраструктура Dallas Lock
ВМ	виртуальная машина
Гипервизор	программа или аппаратная схема, обеспечивающая или позволяющая одновременное, параллельное выполнение нескольких ОС на одном ТС
ДБ	организация единой политики безопасности совокупностью СБ ВИ и агентов управления доступом, работающих под управлением СБ ВИ
Консоль	Консоль Центра управления СЗИ ВИ Dallas Lock. Программное обеспечение для управления Центром управления СЗИ ВИ Dallas Lock

Объект ВИ	объекты виртуальной инфраструктуры Dallas Lock, такие как: СВ vCenter, СВ vCSA, гипервизор ESXi, гипервизор Hyper-V, виртуальная машина
ОС	операционная система
СБ ВИ	сервер безопасности виртуальной инфраструктуры Dallas Lock. Компонент Центра управления СЗИ ВИ Dallas Lock, программная часть которого представляет из себя программную надстройку над сервером УД для возможности работы с объектами ВИ
СВ	сервер виртуализации
Сервер УД	сервер управления доступом. Компонент Центра управления СЗИ ВИ Dallas Lock, с помощью которого осуществляется управление параметрами
СЗИ ВИ	система защиты информации в виртуальных инфраструктурах
ТС	техническое средство
Центр управления СЗИ ВИ Dallas Lock	совокупность программных компонентов АУД, сервера УД и СБ ВИ, управляемая с помощью Консоли

1. НАЗНАЧЕНИЕ

1.1. Изделие предназначено для защиты среды виртуализации на базе VMware vSphere (vCenter for Windows 5.5, 6.0, 6.5, 6.7 и vCSA 6.5, 6.7 совместно с ESXi[1] аналогичной версии) и Microsoft Hyper-V (версий 2012/2012 R2/2016/2019) от несанкционированного доступа при работе в многопользовательских автоматизированных системах (АС), государственных информационных системах (ГИС), в автоматизированных системах управления (АСУ), информационных системах персональных данных (ИСПДн) и при защите значимых объектов критической информационной инфраструктуры (КИИ).

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 включает в себя следующие компоненты:

- ядро системы защиты информации в виртуальных инфраструктурах (далее – Ядро СЗИ ВИ);
- агент управления доступом (далее – АУД);
- сервер управления доступом (далее – Сервер УД);
- агент DL ESXi для гипервизора ESXi;
- агент DL vCenter for Windows для сервера виртуализации vCenter;
- агент DL vCSA для сервера виртуализации vCSA;
- агент DL Hyper-V для гипервизора Hyper-V.

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 6.0/6.5/6.7 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.

ТС с установленным VMware vCSA 6.5/6.7 должно 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.

ТС с установленным гипервизором VMWare ESXi 6.0/6.5/6.7 должно 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.

ТС с установленным Microsoft Hyper-V (версий 2012, 2012 R2, 2016, 2019) должно иметь следующий состав и характеристики программно-технического обеспечения:

– процессор: Intel или AMD с 2-мя логическими ядрами по 2 ГГц каждое;
– ОЗУ – минимум 2 Гб;
– ПЗУ – минимум 32 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. Для модуля изделия Сервер УД предусмотрен механизм проверки наличия более новых версий.

2.5. 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.

2.6. 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 информационных системах персональных данных до 1 уровня защищенности (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») (далее – приказ № 21);
- в государственных информационных системах до 1 класса защищённости включительно (Приказ ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну,

содержащейся в государственных информационных системах») (далее – приказ №17);

- при создании защищенных автоматизированных 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»);
- защищённых значимых объектов критической информационной инфраструктуры до первой категории включительно (Приказ ФСТЭК от 25 декабря 2017 г №239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»).

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;
- подсистема гарантированной очистки памяти;
- подсистема контроля целостности;
- подсистема администрирования;
- подсистема восстановления после сбоев;
- подсистема фильтрации трафика;
- подсистема аудита;
- подсистема развертывания (установочные модули).

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 Сервере УД и сервере виртуализации vCenter и гипервизоре Hyper-V. Контроль пользователей, имеющих право на вход на гипервизор ESXi должен осуществляться посредством выполнения необходимых настроек на стороне Сервера УД и процесса синхронизации гипервизора с Сервером УД.

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 Сервера УД и процесса синхронизации гипервизора ESXi с Сервером УД.

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 или гипервизора Hyper-V;
- имя доменного пользователя AD при условии, что Сервер УД, сервер виртуализации vCenter или гипервизор Hyper-V, введены под управление AD и на сервере виртуализации vCenter или гипервизоре Hyper-V подключен контроллер домена в качестве возможного средства проверки авторизации. Вход доменных пользователей возможен только на Сервере УД и сервере виртуализации vCenter или гипервизоре Hyper-V;
- 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 Сервера УД.

3.3.5. Для Сервера УД 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.

3.3.8. Для Сервера УД и сервера виртуализации vCenter и гипервизора Hyper-V реализовано ограничение числа параллельных сеансов доступа для каждой учётной записи пользователя.

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 – Серверу УД, серверу виртуализации vCenter и гипервизору Hyper-V. Разграничение доступа к гипервизорам ESXi и виртуальным машинам ESXi (файлам виртуальных машин) реализуется в пределах ролевой модели разграничения доступа vSphere.

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, сервере виртуализации vCenter и гипервизора Hyper-V. Разграничение доступа к гипервизорам ESXi и виртуальным машинам (файлам виртуальных машин) реализуется в пределах ролевой модели разграничения доступа vSphere.

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 ТС, освобождаемых областей памяти внешних накопителей. Очистка осуществляется однократной произвольной записью в освобождаемую область памяти, ранее использованную для хранения защищаемых данных (файлов). На гипервизорах Hyper-V и 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 Сервере УД и серверах виртуализации vCenter и Hyper-V (периодический, по расписанию, по запросу), на гипервизоре ESXi (периодический, по запросу), на ВМ (периодически, по расписанию, по запросу). 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 фильтрации трафика

3.7.1. Осуществляется фильтрация входящего сетевого трафика.

3.8. Подсистема администрирования

3.8.1. Управление параметрами безопасности для всех защищенных СЗИ ВИ Dallas Lock компонентов виртуальной инфраструктуры осуществляется из единого Центра управления СЗИ ВИ Dallas Lock.

3.9. Подсистема восстановления после сбоев

3.9.1. Имеется возможность сохранения и применения файла конфигурации настроек СБ ВИ из консоли Сервера УД.

3.10. Подсистема аудита

3.10.1. Осуществляется регистрация входа (выхода) субъектов доступа в систему (из системы), либо регистрация загрузки и инициализации операционной системы и ее программного останова (для Сервера УД и серверов виртуализации). 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.

3.10.2. Для всех компонентов виртуальной инфраструктуры с ОС семейства Windows (включая сервер виртуализации vCenter и гипервизор Hyper-V) 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).

3.10.3. Для сервера виртуализации vCenter и гипервизоров Hyper-V и ESXi, в пределах имеющейся информации в журналах, 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.

3.10.4. Для сервера виртуализации vCenter и гипервизоров Hyper-V и ESXi, в пределах имеющейся информации в журналах, 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).

3.10.5. Для всех компонентов виртуальной инфраструктуры реализована возможность определения типов событий безопасности, подлежащих регистрации.

3.10.6. Для Сервера УД реализована возможность определения состава и содержания информации о событиях безопасности, подлежащих регистрации.

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

3.10.8. 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).

3.11. Подсистема развертывания

3.11.1. Осуществляется локальное и удаленное (средствами Консоли) развертывание компонентов защиты СЗИ ВИ Dallas Lock.

3.12. Доработка существующих подсистем

3.12.1. СЗИ ВИ Dallas Lock блокирует подключения к серверу виртуализации vCenter, гипервизорам Hyper-V и ESXi с несанкционированных удаленных консолей.

3.12.2. Осуществляется использование предустановленных шаблонов типовых политик безопасности на основе требований руководящих документов.

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;
- 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 в ядре системы защиты виртуализации в процессе работы, и журналы гипервизоров, анализируемые и собираемые Сервером УД, собственный журнал событий безопасности Сервера УД;
- 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.