ФУНКЦИОНАЛЬНАЯ СПЕЦИФИКАЦИЯ

Дата выпуска:	07.06.2022
Статус документа:	Released
Версия ПО:	2.6

Содержание

1. Информация о документе

1.1. Назначение

Назначение данного документа - описать возможности, предоставляемые системой “Гарда Файлы” (далее Система), требования к обеспечению Системы для её штатного функционирования и варианты развёртывания.

1.2. Область применения

Документ предназначен для ПО “Гарда Файлы” версии 2.6.

1.3. Целевая аудитория

Документ предназначен для сотрудников отдела информационных технологий и служб информационной безопасности организации, сотрудников отдела информационных технологий, в зоне ответственности которых будет установка и контроль штатного функционирования системы “Гарда Файлы”.

1.4. Термины, определения и сокращения

ПО	Программное обеспечение
Система, ПК “Гарда Файлы”	Программный комплекс “Гарда Файлы”
Администратор системы	Сотрудник, обладающий учетной записью с административными привилегиями, отвечающий за настройку и поддержание в рабочем состоянии системы “Гарда Файлы”
Пользователь Системы	Сотрудник, занимающийся мониторингом событий доступа к хранилищам неструктурированных данных, их структуры, а также структуры организации, включающей права доступа.
Файловый сервер	Хранилище неструктурированных данных под управлением ОС Windows/Linux
Почтовый сервер	Сервер пересылки и хранения электронных почтовых сообщений
ОС	Операционная система - комплекс взаимосвязанных программ, предназначенных для управления ресурсами компьютера и организации взаимодействия с пользователем
Браузер	Программное средство навигации и просмотра ресурсов сети интернет

ИТ / IT	Информационные технологии
ИБ	Информационная безопасность
SIEM-система	Система предназначенная для сбора и анализа информации, поступающей из различных источников с целью выявления отклонений по заданным критериям
Syslog	Стандарт отправки и регистрации сообщений о происходящих в системе событиях (то есть создания событийных журналов), использующийся в компьютерных сетях, работающих по протоколу IP.
TCP	Один из основных протоколов передачи данных интернета, предназначенный для управления передачей данных.
UDP	Один из ключевых элементов набора сетевых протоколов для Интернета. С UDP компьютерные приложения могут посылать сообщения (в данном случае называемые датаграммами) другим хостам по IP-сети без необходимости предварительного сообщения для установки специальных каналов передачи или путей данных.
HTTP	(HyperText Transfer Protocol) Протокол прикладного уровня передачи данных
JSON	Текстовый формат обмена данными, основанный на стандарте ECMA-262 1999 года.
Стороннее ПО	Программное обеспечение разработанное независимыми разработчиками и не по заказу ООО «Гарда Технологии»; к нему относится операционные системы, различные прикладные приложения, ПО управление файловыми хранилищами и т.д.

2. Функциональные возможности

2.1. Назначение системы

“Гарда Файлы” – это комплекс класса DAG (Data Access Governance), позволяющий осуществлять мониторинг операций пользователей с данными, хранящимися на файловых серверах и почтовых серверах под управлением ОС Windows Server (далее – защищаемые сервера). Система также позволяет сканировать и классифицировать сервера, операции с которыми она контролирует, получать структуру каталогов/файлов с неограниченным уровнем вложенности, получать права доступа пользователей к данным содержащимся на защищаемых серверах и выявлять подозрительную активность при доступе к данным.
Комплекс предназначен для решения задач представителей информационной безопасности и IT подразделений организаций.

2.2. Архитектура и состав Системы

Система «Гарда Файлы» состоит из следующих функциональных частей:

- Модуль мониторинга доступа к серверам с защищаемой информацией
  Данный модуль позволяет осуществлять фиксацию всех операций с данными, происходящими на защищаемых серверах, таких как: Чтение, Удаление, Переименование, Копирование и др., а также, в ряде случаев, выполнять активные действия для предотвращения развития потенциальных инцидентов информационной безопасности. В зависимости от типа защищаемого сервера модуль может быть представлен в виде
    - агентского решения,
    - модуля получения информации средствами штатного аудита.

- Модуль аудита MS ActiveDirectory
  Модуль осуществляет фиксацию событий, связанных с функционированием MS ActiveDirectory: создание/изменение/удаление учетных записей и других объектов, факты успешной и неуспешной авторизации, блокировки, активации, отключения учетных записей и др.

- Модуль анализа и сохранения событий аудита
  Модуль осуществляет анализ, обогащение и сохранение событий, зафиксированных модулями мониторинга доступа к серверам.

- Модуль получения структуры и прав доступа к защищаемым серверам
  Модуль позволяет получать и представлять пользователям системы двунаправленную модель доступа к данным.

- Модуль классификации данных защищаемых серверов

Модуль позволяет получать информацию о наличии той или иной критичной информации в файлах, содержащихся на защищаемых хранилищах, такой как: кредитные карты, ПДН, финансовая информация, и другое.

- Модуль выявления аномалий
  Модуль предназначен для обнаружения в автоматическом режиме нетипичной активности на хранилищах, а также аномальных действий отдельно взятых сотрудников.

- Модуль выявления инцидентов, уведомлений и интеграции с внешними системами
  Модуль позволяет выявлять ситуации, свидетельствующие о наличии риска ИБ (инциденты) согласно заданным правилам, оперативно информировать об этом, отправляя системные события в другие системы (например, SIEM-системы), а также осуществлять уведомления по электронной почте сотрудников компании.

- Модуль управления системой
  Модуль предоставляет пользовательский интерфейс для управления системой и анализа полученных данных.

- Модуль поиска по содержимому файлов
  Модуль предоставляет возможность быстрого поиска по содержимому файлов, находящихся на защищаемых хранилищах.

- Модуль самодиагностики системы
  Модуль осуществляет мониторинг основных работы системы, а также параметры функционирования ОС.

2.3. Функциональные возможности

2.3.1. Основные функции

Система “Гарда Файлы” позволяет осуществлять мониторинг операций пользователей с данными, хранящимися на файловых серверах и почтовых серверах. К основным функциям Системы относится:

- Мониторинг действий сотрудников с информацией, находящейся на хранилищах неструктурированных или слабоструктурированных данных:
  - файловых серверах под управлением ОС MS Windows Server 2008 и выше
  - файловых серверах под управлением ОС на базе Linux
  - почтовых серверах MS Exchange
  - MS SharePoint
  - различных Системы Хранения Данных (Dell EMC, NetApp и др.)
  - и др.

- Предоставление информации о полной структуре файлов/каталогов защищаемых серверов с автоматической фиксации потенциальных рисков и угроз ИБ, связанных с назначением прав на файлы и каталоги
- Классификация данных контролируемых серверов
- Предоставление двунаправленной картины прав пользователей к данным контролируемых серверов
- Обеспечение длительного хранения информации об операциях с документами и файлами, расположенными на контролируемых серверах
- Поиск по результатам аудита (операций с данными защищаемых систем)
- Выявление нетипичной активности на контролируемых серверах и аномального поведения сотрудников относительно данных, находящихся на контролируемых серверах
- Фиксация ситуаций, свидетельствующих о повышенном риске ИБ (подозрения на инциденты) согласно заданным правилам
- Предоставление средств активного подавления распространения инцидента

3. Требования к обеспечению

3.1. PM пользователя Системы

Графический интерфейс пользователя Системы выполнен в виде веб-приложения. Доступ к интерфейсу осуществляется с использованием одного из следующих веб-браузеров:

- Google Chrome версии 60.0.3112 и выше;
- Mozilla Firefox версии 52 и выше;
- Microsoft Edge;
- Яндекс.Браузер версии 17.6.1 и выше

Операционная система, на которой запускается веб-браузер, может быть любой из поддерживаемых конкретной версией браузера.

3.2. Сервер Системы

3.2.1. Программное обеспечение

Серверное ПО “Гарда Файлы” может функционировать в следующих операционных системах:

- Ubuntu Server 18.04, 20.04
- CentOS 7.4 - 7.9
- Red Hat Enterprise Linux 7.4 - 7.9
- Astra Linux релиз Orel 2.12 и выше

Выбор операционной системы, в которой будет функционировать серверное ПО “Гарда Файлы” зависит от принятых в организации стандартов и политик.
Если нет ограничений относительно представленных выше ОС, производителем рекомендуется использовать Ubuntu Server.

Установку ОС следует производить согласно стандартным инструкциям, прилагающимся к каждой из вышеперечисленных ОС и доступным по следующим ссылкам:

- Ubuntu Server: https://tutorials.ubuntu.com/tutorial/tutorial-install-ubuntu-server#0
- CentOS: https://docs.centos.org/en-US/centos/install-guide/
- Red Hat Enterprise Linux 7: https://access.redhat.com/documentation/ru-ru/red_hat_enterprise_linux/7/html/installation_guide/index
- Astra Linux Орел 2.12: https://wiki.astralinux.ru/pages/viewpage.action?pageId=37290417

3.2.2. Аппаратное обеспечение

Программное обеспечение системы “Гарда Файлы” может функционировать на физических серверах и виртуальных машинах.
Минимальные требования к выделяемым ресурсам:

Без модуля поиска:

- Количество ядер процессора: 8 с тактовой частотой не менее 2.0 ГГц
    - Процессор должен поддерживать следующие инструкции: SSE, SSE2, SSE4_2, AVX
- Объем оперативной памяти: 16 Гб
- Объем жесткого диска: 100 Гб

С модулем поиска, установленном там же, где и другие серверные компоненты “Гарда Файлы”:

- Количество ядер процессора: 10 с тактовой частотой не менее 2.0 ГГц
    - Процессор должен поддерживать следующие инструкции: SSE, SSE2, SSE4_2, AVX
- Объем оперативной памяти: 20 Гб
- Объем жесткого диска: 200 Гб

Для отдельно установленного узла сканирования в случае кластерного варианта:

- Количество ядер процессора: 4 с тактовой частотой не менее 2.0 ГГц
    - Процессор должен поддерживать следующие инструкции: SSE, SSE2, SSE4_2, AVX
- Объем оперативной памяти: 8 Гб
- Объем жесткого диска: 50 Гб

Для отдельно установленного узла индексации и поиска:

- Количество ядер процессора: 4 с тактовой частотой не менее 2.0 ГГц
    - Процессор должен поддерживать следующие инструкции: SSE, SSE2, SSE4_2, AVX
- Объем оперативной памяти: 4 Гб
- Объем жесткого диска: 100 Гб

Сервер должен быть подключен к сети организации.
Для сервера необходимо выделить IP-адрес и доменное имя.

3.3. Агентское ПО “Гарда Файлы”

Агентское ПО “Гарда Файлы” может быть установлено на следующие операционные системы:

- MS Windows Server 2012 R2 и выше
- MS Windows XP и выше
- Ubuntu Server 18.x
- RHEL/Centos 7.x
- Astra Linux Орел 2.12