ГАРДА
ТЕХНОЛОГИИ

ООО "Гарда Технологии"

Руководство администратора

Модуль Хранилище ПК "Периметр"

Нижний Новгород, 2022

Оглавление

1 Введение

1.1 Аннотация

Данный документ представляет собой Руководство администратора к программному модулю «Хранилище», входящий в состав программного обеспечения ПРОГРАММНЫЙ КОМПЛЕКС «ПЕРИМЕТР».

1.2 Термины, определения и сокращения

Термин	Значение
ПК	ПРОГРАММНЫЙ КОМПЛЕКС «ПЕРИМЕТР»
Система	ПК «ПЕРИМЕТР»
Модуль	Модуль «Хранилище»
СПД	Сеть передачи данных
БРП	База решающих правил
DoS	Сетевая (компьютерная) атака, направленная на отказ в обслуживании
DDoS	DoS-атака, выполняемая одновременно с большого числа компьютеров

1.3 Использование имен, номеров телефонов, сетевых адресов

Все регистрационные имена пользователей, а также номера телефонов, имена и другие данные абонентов, используемые в Руководстве, являются вымышленными, а IP-адреса не соответствуют их действительным владельцам. Любые совпадения случайны.

1.4 О компании

«Гарда Технологии» – российский разработчик систем защиты от внутренних и внешних угроз информационной безопасности, противодействия мошенничеству и расследования инцидентов. Решения «Гарда Технологии» занимают лидирующие позиции на российских рынках решений информационной безопасности.

Разработки аппаратно-программных решений информационной безопасности ведутся с 2005 года. Исследовательский центр компании обладает 5 патентами на уникальные технологии. Решения «Гарда Технологии» внедрены в крупнейших компаниях финансового сектора, промышленных предприятиях, операторах связи и государственных структурах России и СНГ. Подробнее – на gardatech.ru

1.5 Техническая поддержка

По всем вопросам, связанным с работой продукта, обращайтесь в Службу технической поддержки компании «Гарда Технологии»:

- Тел. +7 (831) 422-12-20 (с 9-00 до 18-00 по Московскому времени).
- Email: ddos.support@gardatech.ru

2 Назначение Системы

ПРОГРАММНЫЙ КОМПЛЕКС «ПЕРИМЕТР» (далее ПК «ПЕРИМЕТР») представляет собой систему обнаружения и противодействия сетевым атакам типа «Отказ в обслуживании DoS/DDoS» (далее DDoS) и анализа трафика на сети передачи данных (далее СПД).

Решение данной задачи основано на:

- постоянном контроле состояния трафика СПД и его многостороннем анализе;
- обнаружении отклонений параметров трафика (аномалий);
- интеллектуальной фильтрации трафика с блокированием вредоносной составляющей и пропуском легитимной.

3 Установка модуля «Хранилище»

3.1 Развертывание комплекса

В рамках развертывания комплекса необходимо произвести приемку согласно комплектности поставки и проверку информации, записанной на оптический диск установочного комплекта.

Для функционирования ПК «Периметр» необходимо установить операционную систему Debian 10.0. Дистрибутив доступен на официальном сайте (https://cdimage.debian.org/cdimage/archive/10.7.0/amd64/iso-cd/). Поддерживаемая архитектура - amd64, поддерживаемая версия ядра системы - 4.19.0-6-amd64.

Действия по формированию функциональной среды требуют наличие прав суперпользователя.

После разметки дискового пространства и установки необходимых для функционирования используемой аппаратной платформы драйверов и утилит, выполняется установка модуля «Хранилище» с помощью менеджера пакетов:

```
- для Debian 10:

  apt-get install --assume-yes --allow-unauthenticated -o DPkg::Options::="--force-
↪overwrite" synflowstorage_5.58854P_amd64.deb

- для AltLinux 8SP:

  apt-get install --assume-yes --allow-unauthenticated -o DPkg::Options::="--force-
↪overwrite" synflowstorage-5.58854P-2.x86_64.rpm
```

После установки модуля «Хранилище» все его компоненты запускаются автоматически.

3.2 Настройка модуля «Хранилище»

Настройка производится с помощью конфигурационных файлов модулей «Хранилище» и «Анализатор».

Для корректной работы модуля требуется настроить следующие параметры:

- USERNAME
- PASSWORD
- DB_NAME
- DB_TABLE
- DB_ADDR
- DB_PORT
- BLOCK_SIZE
- QUEUE_SIZE

Далее требуется инициализировать базу данных согласно схемы, представленной разработчиком.

4 Обновление модуля «Хранилище»

Предприятие-разработчик на этапе сопровождения может осуществлять периодический выпуск обновлений.

Определены три типа обновлений Изделия:

- 1 тип – обновление баз данных, необходимые для поддержания актуальности БРП;
- 2 тип – обновление, направленное на устранение выявленных уязвимостей (критическое обновление) ПК;
- 3 тип – обновление, направленное на добавление и/или совершенствование реализации функций безопасности, на расширение числа поддерживаемых программных и аппаратных платформ (обновление версии ПК).

Информирование потребителей о выпуске обновлений Изделия 2 и 3 типа осуществляется путем рассылки информационных уведомлений потребителям Изделия.

Обновление модуля «Анализатор» осуществляется с помощью менеджера пакетов.