Программное средство обнаружения компьютерных атак «ЗАСТАВА-IDS», версия 1

Функциональные характеристики

2022

СОДЕРЖАНИЕ

1. ОБЩИЕ СВЕДЕНИЯ

1.1. Наименование изделия и условное обозначение

1.1.1. Наименование изделия – программное средство обнаружения компьютерных атак «ЗАСТАВА-IDS», версия 1 (далее – СОА «ЗАСТАВА-IDS»).

1.1.2. Условное обозначение – СОА «ЗАСТАВА-IDS».

1.2. Разработчик

Акционерное общество «ЭЛВИС-ПЛЮС».

124527, Москва, Зеленоград, Солнечная аллея, д. 6, помещение VI, офис 7, тел. (495) 276-0211.

1.3. Поставщик

Акционерное общество «ЭЛВИС-ПЛЮС».

124498, Москва, Зеленоград, Солнечная аллея, дом 6, тел. (495) 276-0211.

1.4. Модификация

СОА «ЗАСТАВА-IDS».

2. ОСНОВНЫЕ ХАРАКТЕРИСТИКИ

2.1. СОА «ЗАСТАВА-IDS» предназначен для обнаружения в информационных системах в автоматическом режиме компьютерных атак на основе анализа сигнатурным методом сетевого трафика стека протоколов TCP/IP.

2.2. СОА «ЗАСТАВА-IDS» имеет механизмы обнаружения компьютерных атак на основе анализа протоколов всех уровней модели взаимодействия открытых систем или 5-уровневой модели TCP/IP начиная с сетевого.

2.3. СОА «ЗАСТАВА-IDS» состоит из двух основных компонентов – сетевого сенсора и центрального сервера.

2.4. Сетевой сенсор предназначен для поиска компьютерных атак в сетевом трафике.

2.5. Центральный сервер обеспечивает управление подключенными сетевыми сенсорами, а также сбор с них и отображение администратору комплекса информации об обнаруженных компьютерных атаках.

3. РАСШИРЕННЫЕ ФУНКЦИОНАЛЬНЫЕ ХАРАКТЕРИСТИКИ

3.1. СОА «ЗАСТАВА-IDS» имеет графический веб-интерфейс для удобного и наглядного конфигурирования и мониторинга.

3.2. В СОА «ЗАСТАВА-IDS» предусмотрен механизм регистрации и идентификации данного события, а также непосредственной сигнализации о нём администратору путём визуального отображения соответствующего сообщения на консоли управления.

3.3. В СОА «ЗАСТАВА-IDS» предусмотрен механизм отсылки сообщений электронной почты при наступлении определённых событий, наиболее критичных для контролируемой системы.

3.4. СОА «ЗАСТАВА-IDS» имеет механизмы настройки выборочного контроля ресурсов информационной системы на уровне отдельных объектов сети.

3.5. СОА «ЗАСТАВА-IDS» имеет механизм, позволяющий осуществлять как локальное, так и удалённое управление (администрирование) данным средством

3.6. СОА «ЗАСТАВА-IDS» имеет механизм, обеспечивающий маскирование наличия сенсора указанного средства в составе контролируемой информационной системы и невыявления его на сетевом уровне стандартными средствами операционных систем, в средах которых функционирует указанное средство.

3.7. СОА «ЗАСТАВА-IDS» обеспечивает идентификацию и аутентификацию администратора данного средства при его локальных запросах на доступ к процессу управления по идентификатору (коду) и/или паролю.

3.8. СОА «ЗАСТАВА-IDS» имеет автоматизированный механизм обновления базы сигнатур компьютерных атак и его программных модулей.

3.9. В СОА «ЗАСТАВА-IDS» реализованы штатные средства задания новых сигнатур при предоставлении новой версии указанной базы.

3.10. В СОА «ЗАСТАВА-IDS» реализован механизм автоматической регистрации и хранения информации о следующих событиях:

- для выявленных атак: протокол, используемый для проведения атаки, идентификатор субъекта атаки (если его можно определить на основе анализа трафика), идентификатор объекта атаки, код регистрируемого события, результат попытки осуществления регистрируемого события (если его можно определить на основе анализа трафика);
- факт вход/выхода администратора СОА «ЗАСТАВА-IDS» и его идентификатор, а также результаты проведения идентификации и аутентификации при доступе для управления;
- момент запуска СОА «ЗАСТАВА-IDS» при включении/перезагрузке объекта контролируемой информационной системы, на котором установлено данное средство;
- результатов проверки целостности программной части и настроек данного средства.