УТВЕРЖДЕН
ДБАР.62.01.12.000.181-01 34-ЛУ

ПК «СОВ «ПЛУТОН-М1.0»

Руководство оператора

ДБАР.62.01.12.000.181-01 34

Листов 27

Инв.№ подл.	Подп. и дата	Взам.инв.№	Инв.№ дубл.	Подп. и дата

Москва
2018

АННОТАЦИЯ

Настоящий документ является руководством оператора ДБАР.62.01.12.000.181-01 34.

В документе определены основные задачи и функции программы, рассмотрены назначение, условия выполнения программного комплекса «Система обнаружения вторжений «Плутон-М1.0» (ПК «СОВ «Плутон-М1.0»), далее по тексту – ПК СОВ, СОВ). Приведена методика работы операторов (пользователей программы) в графическом пользовательском интерфейсе, типовые приёмы работы и сообщения оператору.

СОДЕРЖАНИЕ

1 НАЗНАЧЕНИЕ ПРОГРАММЫ

1.1 Назначение программы

Программный комплекс «Система обнаружения вторжений «Плутон-М1.0» (далее – ПК СОВ) предназначен для:

– обнаружения угроз безопасности информации, относящихся к вторжениям (атакам);

– защиты информации в информационных системах;

– сбора статистических данных трафика в контролируемых системах;

– сбора информации о событиях на узлах (хостах) контролируемых систем;

– сбора информации о передаваемых пакетах данных и о событиях, связанных с работой распределённого программного обеспечения, применяемого на узлах контролируемых систем.

1.2 Решаемые задачи

ПК СОВ состоит из двух программных средств (ПС)):

– ПС «Сенсор-Плутон-М1.0» (далее – ПС Сенсор) – программное средство, предназначенное для обнаружения КА, сбора статистики сетевого трафика и информации о хостах контролируемой системы;

– ПС «СУС-Плутон-М1.0» (далее – ПС СУС) – программное средство, предназначенное для управления ПС Сенсор, и системными параметрами, информирования пользователей ПК СОВ о зафиксированных КА в режиме реального времени и вывода статистических данных за заданный интервал времени.

1.2.1 ПС Сенсор выполняет следующие функции:

1) Регистрация и идентификация сетевых вторжений на основе анализа сетевого трафика, передаваемого по контролируемому каналу связи.

2) Сбор информации об операционных системах, распределённом программном обеспечении, учётных записях пользователей, сертификатах хостов контролируемой системы.

3) Обнаружение отклонений от эталонных профилей хостов контролируемых систем (обнаружение или изменение операционной системы, распределённого программного обеспечения, учётных записей пользователей, сертификатов).

4) Накопление информации о выявленных сетевых вторжениях в автономном режиме при отсутствии связи с ПС СУС и передача накопленной информации при восстановлении связи.

5) Контроль свободного дискового пространства, архивирование и автоматическое удаление устаревшей информации при переполнении жёсткого диска.

6) Регистрация событий аудита безопасности.

7) Фиксация, передача и обеспечение гарантированной доставки на ПС СУС:

– данных зарегистрированных сетевых вторжений – событий информационной безопасности (далее – СИБ);

– статистических характеристик сетевого трафика, передаваемого по контролируемому каналу передачи данных;

– параметров функционирования технических и программных средств ПС Сенсор;

– данных аудита безопасности ПС Сенсор;

– копии трафика;

– данных о сетевых взаимодействиях узлов контролируемых систем;

– данных о распределённом программном обеспечении узлов контролируемых систем.

8) Агрегация однотипных событий.

9) Предоставление пользователям возможности настроить ПС Сенсор и изменить его параметры конфигурирования с помощью командной среды операционной системы (ОС).

10) Выполнение команд, поступающих из ПС СУС.

11) Регулирование доступа пользователей к функциям ПС Сенсор в соответствии с настройками ролевой модели доступа. В поставке ПК СОВ предусмотрена роль «Администратор безопасности СОВ», которая разрешает выполнять команды настройки и конфигурирования ПС Сенсор с помощью командной среды ОС.

12) Идентификация, аутентификация и авторизация пользователей выполняется посредством операционной системы. При этом:

– для доступа используются логины и пароли пользователей;

– отслеживается выполнение требований к сложности пароля (длина, специальные символы, цифры, буквы в верхнем и нижнем регистре) и к периодичности смены пароля.

13) Взаимодействие ПС Сенсор с ПС СУС по защищённому каналу связи. Для исключения несанкционированного доступа во время установки соединения удалённый компонент идентифицируется с помощью проверки цифрового сертификата.

14) Обновление ПС Сенсор в части базы решающих правил сигнатурного анализа, чёрных списков, программных сценариев эвристического анализа, справочников, базы уязвимости, базы GeoIP и программного обеспечения.

15) Маскирование своего функционирования за счёт применения механизмов операционной системы.

1.2.2 Функции ПС СУС

ПС СУС выполняет следующие функции:

1) Поддержка иерархической модели подчинения компонентов ПС СУС и ПС Сенсор.

2) Предоставление пользователю возможности анализировать данные, как поступающих с подчинённых компонентов, так генерируемых самим ПС СУС с помощью графического пользовательского интерфейса.

3) Приём от ПС Сенсор, хранение и передача на вышестоящий ПС СУС:

– СИБ;

– статистических характеристик сетевого трафика, передаваемого по контролируемому каналу передачи данных;

– параметров функционирования технических и программных средств – своих и подчинённых компонентов;

– данных аудита безопасности – своих и подчинённых компонентов;

– копий трафика;

– данных о распределённом программном обеспечении узлов контролируемых систем.

4) Накопление информации об эталонных профилях хостов контролируемых систем и передача их на ПС Сенсор.

5) Регистрация событий аудита безопасности.

6) Предоставление пользователям возможности настроить ПС СУС и подчинённые компоненты и изменить параметры их конфигураций с помощью командной среды ОС и графического пользовательского интерфейса.

7) Выполнение команд, поступающих из вышестоящего ПС СУС.

8) Регулирование доступа пользователей к функциям ПС СУС в соответствии с настройками ролевой модели доступа. В поставке ПК СОВ предусмотрены:

– роль «Администратор безопасности СОВ», которая разрешает настраивать ПС СУС и подчинённые компоненты и изменять параметры конфигураций с помощью командной среды ОС и графического пользовательского интерфейса;

– роль «Оператор визуального контроля СОВ», которая разрешает выполнять:

a) анализ СИБ,

b) анализ собственных событий аудита безопасности и событий аудита безопасности подчиненных компонентов

c) анализ собственного состояния и состояний подчиненных компонентов

d) настройку решающие правила сигнатурного анализа.

9) Идентификация, аутентификация и авторизация пользователей выполняется через механизмы операционной системы. При этом:

– для доступа используются логины и пароли пользователей;

– отслеживается выполнение требований к сложности пароля (длина, специальные символы, цифры, буквы в верхнем и нижнем регистре) и к периодичности смены пароля.

10) Взаимодействие программных средств ПК СОВ по защищённому каналу связи. Для исключения несанкционированного доступа во время установки соединения удалённый компонент идентифицируется с помощью проверки ЭП.

11) Взаимодействие с внешней системой обновлений.

12) Обновление ПС СУС в части базы решающих правил сигнатурного анализа, чёрных списков, справочников, базы уязвимости, базы GeoIP, данных картографии, программного обеспечения и передача обновлений на подчинённые компоненты.

Предоставление данных СИБ в формате CEF (Common Event Format) для передачи во внешние SIEM-системы.

1.3 Состав программы

1.3.1 Модуль «Графический пользовательский интерфейс»

Модуль представляет собой веб-приложение, работающее в среде браузера и защищённое протоколом HTTPS. Модуль предоставляет графический пользовательский интерфейс (ГПИ) к функциям ПК СОВ и позволяет:

– просматривать, фильтровать и проводить поиск данных о СИБ, событиях аудита безопасности, событиях системы обнаружения атак (СОА);

– просматривать статистику контролируемого сетевого трафика в виде графиков и диаграмм;

– просматривать данные мониторинга компонентов, профилей хостов, топологии сети;

– просматривать КА и местоположение объектов ПК СОВ на географической карте;

– просматривать решающие правила сигнатурного анализа и чёрные списки;

– выполнять настройки компонентов ПК СОВ и параметров контролируемых систем;

– управлять пользователями ПК СОВ и настраивать ролевую модель доступа;

– инициировать команды регистрации компонентов, активирования/деактивирования компонентов и решающих правил сигнатурного анализа и чёрных списков, подтверждения данных профиля хоста.

1.3.2 Модуль «Захват и буферизация»

Модуль выполняет захват и кольцевую буферизацию сетевого трафика помощью программного интерфейса операционной системы AF_PACKET. ПК СОВ может работать в режимах:

– разрыв канала;

– прослушивание канала (использует копию сетевого трафика).

1.3.3 Модуль «Сигнатурный анализ»

Модуль выполняет сигнатурный анализ пакетов сетевого трафика, формирует СИБ и журналы событий СОА. Сигнатурный анализ реализуется с помощью СОА Suricata, СОА Bro и утилиты p0f.

Правила сигнатурного анализа хранятся в виде файлов. Хранение данных обеспечивает модуль «Хранение файлов».

1.3.4 Модуль «Эвристический анализ»

Модуль:

– выявляет новые хосты в контролируемой системе;

– выявляет новое ПО на хостах контролируемой системы;

– обнаруживает в сетевом трафике те атрибуты сущностей, которые включены в чёрные списки;

– в режиме обучения собирает данные о профилях хостов контролируемой системы.

Модуль использует СОА Bro. Программные сценарии эвристического анализа хранятся в виде файлов. Хранение данных обеспечивает модуль «Хранение файлов».

1.3.5 Модуль «Сбор статистики»

Модуль выполняет сбор статистики пакетов сетевого трафика с учётом входящих/исходящих потоков данных с разделением по хостам контролируемой системы ПК СОВ, по портам и протоколам. Собранная статистика используется для анализа аномалий действий хостов контролируемой системы. Данные статистики хранятся в базе данных (БД) ПК СОВ. Хранение обеспечивает модуль «Хранение больших данных».

1.3.6 Модуль «Копирование пакетов»

Для СИБ модуль создаёт копию трафика в виде PCAP-файла[1)]. PCAP-файл содержит информацию: о сетевом пакете, вызвавшем срабатывание решающего правила и десяти пакетах после этого пакета – при их наличии в сетевом соединении. Дополнительная информация для СИБ расширяет возможности расследования СИБ. Хранение копий пакетов обеспечивает модуль «Хранение файлов».

1.3.7 Модуль «Аудит безопасности»

Модуль предназначен для выполнения контролирующих действий и регистрации событий ПК СОВ, которые потенциально могут быть опасными для работоспособности ПК СОВ.

---

1) PCAP-файл создаётся только для сигнатурных событий Suricata

Модуль выполняет:

– аудит целостности, при котором выявляются несанкционированные изменения объектов ПК СОВ (ПО, конфигурационные файлы, база решающих правил сигнатурного анализа, чёрные списки, программные сценарии эвристического анализа);

– аудит действий пользователей ПК СОВ;

– аудит изменений режимов работы ПК СОВ;

– аудит выполнение программ и процессов ПК СОВ.

Аудит целостности использует базу контроля целостности (БКЦ), которая содержит контрольные суммы объектов ПК СОВ. Хранение БКЦ обеспечивает модуль «Хранение файлов». Для аудита целостности применяется утилита Afick.

Модуль выполняет аудит целостности ПК СОВ:

– при старте ПК СОВ;

– по расписанию в соответствии с установленными временными интервалами;

– по команде администратора безопасности СОВ.

Модуль инициирует уведомление пользователей ПК СОВ о событиях аудита. Уведомления формируются и отправляются на адреса электронной почты пользователей в соответствии с настройками.

Модуль выполняет обновление БКЦ.

К событиям аудита безопасности относятся:

– запуск и завершение выполнения функций аудита безопасности;

– запуск и завершения самотестирования;

– запуск и завершение программ и процессов ПК СОВ;

– изменение режимов выполнения функций ПК СОВ;

– попытка удаления СИБ и событий аудита безопасности;

– вход и выход пользователей ПК СОВ;

– неуспешные попытки входа пользователей ПК СОВ;

– изменение настроек ролевой модели доступа к функциям ПК СОВ;

– изменение учётной записи пользователя и изменение пароля пользователя;

– изменение полномочий пользователей ПК СОВ.

Хранение событий аудита безопасности в БД ПК СОВ обеспечивает модуль «Хранение больших данных».

1.3.8 Модуль «Обогащение СИБ»

Модуль предназначен для буферизации и обогащения сырых данных СИБ дополнительной информацией, которая содержится:

- в базах решающих правил сигнатурного анализа;
- в чёрных списках;
- в профилях хостов;
- в справочниках,
- в базе уязвимостей,
- в базе GeoIP.

1.3.9 Модуль «Мониторинг состояний»

Модуль отслеживает состояние и работоспособность ПК СОВ, а также выполняет самотестирование работоспособности ПК СОВ:

- при старте ПК СОВ;
- по расписанию в соответствии с установленными временными интервалами;
- по команде администратора безопасности СОВ.
- Модуль использует в своей работе программу-агент Net-SNMP для мониторинга состояния и работоспособности ПК СОВ. Пользователь может включить дополнительное средство мониторинга работоспособности компонентов Zabbix, входящее в состав поставки ПК СОВ.

Показатели состояния и работоспособности сохраняются в БД ПК СОВ. Для хранения используется модуль «Хранение мастер-данных».

Данные мониторинга используются для определения следующих показателей работоспособности:

- процент использования оперативного запоминающего устройства (ОЗУ);
- процент использования центрального процессорного устройства (ЦПУ);
- процент использования файла подкачки;

– процент использования накопителя на жёстких магнитных дисках (НЖМД);

– признак компрометации ПК СОВ.

1.3.10 Модуль «Обновление»

Модуль выполняет обновление и импорт в БД ПК СОВ обновлённой информации.

Обновление некорневого ПС СУС.

Модуль отслеживает публикации обновлений в вышестоящем ПС СУС. При наличии обновлений модуль скачивает сжатые файлы обновлений (за исключением справочников) и распаковывает их.

Модуль устанавливает файлы обновлений:

– базы GeoIP;

– данных картографии;

– программного обеспечение ПС СУС.

Хранение данных обеспечивает модуль «Хранение файлов».

Модуль импортирует данные следующих обновлений в БД ПС СУС:

– база решающих правил сигнатурного анализа;

– чёрные списки;

– база уязвимости.

Хранение импортируемых данных обеспечивает модуль «Хранение мастер-данных».

Обновление справочных данных выполняет модуль «Передача и приём данных и команд» Справочные данные передаются из БД вышестоящего ПС СУС в БД ПС СУС.

Обновление корневого ПС СУС.

Модуль выполняет регистрацию на сервере обновлений и проводит мониторинг публикации обновлений на сервере обновлений посредством HTTP-запросов. При наличии обновлений модуль скачивает сжатые файлы обновлений (за исключением справочников) и распаковывает их.

Модуль устанавливает файлы обновлений:

– базы GeoIP;

– данных картографии;

– программного обеспечение ПС СУС.

Хранение данных обеспечивает модуль «Хранение файлов».

Модуль импортирует данные следующих обновлений в БД ПС СУС:

– база решающих правил сигнатурного анализа;

– чёрные списки;

– база уязвимости.

Хранение импортируемых данных обеспечивает модуль «Хранение мастер-данных».

Обновление ПС Сенсор

Модуль отслеживает публикации обновлений в ПС СУС и при наличии обновлений скачивает сжатые файлы обновлений (за исключением справочников) и распаковывает их.

Модуль устанавливает файлы обновлений:

– базы решающих правил сигнатурного анализа;

– чёрных списков;

– программных сценариев эвристического анализа;

– базы GeoIP;

– программного обеспечение ПС Сенсор.

Хранение данных обеспечивает модуль «Хранение файлов».

Модуль импортирует данные следующих обновлений в БД ПС Сенсор:

– база решающих правил сигнатурного анализа;

– чёрные списки;

– база уязвимости.

Хранение импортируемых данных обеспечивает модуль «Хранение мастер-данных».

Обновление справочных данных

Обновление справочных данных выполняет модуль «Передача и приём данных и команд». Справочные данные передаются из БД ПС СУС в БД подчинённого компонента. Модуль «Хранение больших данных»

Модуль используется для хранения следующих видов данных:

– СИБ;

– журналы событий СОА;

– события аудита безопасности;

– статистика сетевого трафика.

Модуль использует для хранения систему управления базами данных (СУБД) ClickHouse, которая обладает необходимыми характеристиками производительности чтения и добавления больших данных.

Модуль поддерживает функции:

– резервного копирования БД по расписанию или по команде администратора безопасности СОВ;

– восстановление данных БД из резервной копии;

– архивирование;

– удаление исторических данных.

1.3.11 Модуль «Хранение больших данных»

Модуль используется для хранения следующих видов данных:

– СИБ;

– журналы событий СОА;

– события аудита безопасности;

– статистика сетевого трафика.

Модуль использует для хранения СУБД ClickHouse, которая обладает необходимыми характеристиками производительности чтения и добавления больших данных. Структура и атрибутивный состав данных представлены в документе "ПК «СОВ «Плутон-М1.0». Пояснительная записка. Приложение В Описание структуры базы данных", ДБАР.62.01.12.000.181-01 81-В.

Модуль поддерживает функции:

– резервного копирования БД по расписанию или по команде администратора безопасности СОВ;

– восстановление данных БД из резервной копии;

– архивирование;

– удаление исторических данных.

1.3.12 Модуль «Хранение мастер-данных»

Модуль используется для хранения следующих видов данных:

– профили хостов;

– база решающих правил сигнатурного анализа;

– чёрные списки;

– справочники;

– база уязвимостей.

Модуль использует для хранения СУБД PostgreSQL, которая обладает необходимыми характеристиками для чтения, добавления, изменения, удаления данных с возможностью поддержки транзакционной целостности.

Модуль поддерживает функции:

– резервного копирования БД по расписанию или по команде администратора безопасности СОВ;

– восстановление данных БД из резервной копии;

– архивирование;

– удаление исторических данных.

1.3.13 Модуль «Хранение файлов»

Модуль решает задачи хранения в файловой системе ОС ПК СОВ:

– файлов решающих правил сигнатурного анализа (только для ПС Сенсор);

– файлов чёрных списков (только для ПС Сенсор);

– файлов программных сценариев эвристического анализа (только для ПС Сенсор);

– PCAP-файлов;

– файлов базы GeoIP;

– файлы данных картографии (только для ПС СУС);

– файлов обновлений.

Модуль поддерживает функции:

– резервного копирования по расписанию или по команде администратора безопасности СОВ;

– восстановление данных из резервной копии;

– архивирование;

– удаление исторических данных.

1.3.14 Модуль «Выполнение команд»

Модуль обеспечивает выполнение команд, которые инициируются:

– из командной среды ОС ПК СОВ (см. перечень команд в документах "ПС «Сенсор-Плутон-М1.0». Руководство системного программиста", ДБАР.62.01.12.000.183-01 32 и "ПС «СУС-Плутон-М1.0». Руководство системного программиста", ДБАР.62.01.12.000.182-01 32);

– из модуля «Графический пользовательский интерфейс» ПС СУС.

Передачу команд от одного компонента к другому компоненту выполняет модуль «Передача и приём данных и команд».

1.3.15 Модуль «Передача и приём данных и команд»

Модуль обеспечивает взаимодействие ПК СОВ. Для реализации функций модуля используется протокол MQTT. Используется шаблон взаимодействия публикации/подписки. Взаимодействие ПК СОВ осуществляется по защищённому каналу связи. Для исключения несанкционированного доступа модуль во время установки соединения идентифицирует удалённый компонент с помощью проверки цифрового сертификата.

Модуль обеспечивает передачу данных:

– из вышестоящего компонента в подчинённый компонент:
  – файлы обновлений;
  – справочники.
– из подчинённого компонента в вышестоящий компонент:
  – СИБ;
  – журналы событий СОА;
  – PCAP-файлы;
  – события аудита безопасности подчинённых компонентов;
  – статистика трафика;
  – профили хостов;

– состояния подчинённых компонентов.

Программный интерфейс взаимодействия компонентов ПК СОВ предоставляется в виде сервисов на стороне ПС СУС. За счёт этого достигнута независимость от реализации клиентов на стороне ПС Сенсор. Формат и структура данных спроектированы таким образом, чтобы обеспечить возможность лёгкого расширения.

1.3.16 Модуль «Уведомления»

Модуль выполняет рассылку уведомлений пользователям ПК СОВ по электронной почте. Рассылка запускается по факту появления СИБ в ПС Сенсор и событий аудита безопасности в ПК СОВ. Можно выбрать следующие настройки уведомлений:

– формирование уведомлений в зависимости от типа события;

– формирование уведомления в зависимости от уровня критичности события;

– формирование списков рассылки.

1.3.17 Другие функции ПК СОВ

ПК СОВ включают в себя сервисы, программные сценарии, команды, реализующие отдельные функции:

– Сервис pluton-job-runner поддерживает запуск процессов ПК СОВ по расписанию.

– Сервис pluton-homenet-control реализует применение параметров контролируемой системы в ПС Сенсор.

– Сервис pluton-service-start реализует запуск процессов ПК СОВ, работающих в фоновом режиме.

– Программный сценарий remove_oldest_data.sh по команде модуля «Мониторинг состояний» выполняет действия, предотвращающие переполнение дискового пространства компонента ПК СОВ.

– Интерфейс командной строки (CLI) pluton [options] выполняет команды, которые используются ПК СОВ и могут быть использованы для выполнения команд из командной строки ОС. С помощью интерфейса командной строки можно:

а) выполнять резервное копирование и восстановление БД ПК СОВ;

б) запускать программный сценарий remove_oldest_data.sh;

в) управлять локальными пользователями ОС;

г) импортировать профили хостов.

Подробно о применении команд см. документы "ПС «Сенсор-Плутон-М1.0». Руководство системного программиста", ДБАР.62.01.12.000.183-01 32 и "ПС «СУС-Плутон-М1.0». Руководство системного программиста", ДБАР.62.01.12.000.182-01 32.

– Сервис pluton-ise-handler на основе данных о СИБ формирует сообщение в формате CEF (Common Event Format) для внешних SIEM-систем.

2 УСЛОВИЯ ВЫПОЛНЕНИЯ ПРОГРАММЫ

2.1 Состав технических средств, необходимый для функционирования ПК СОВ

ПК СОВ работоспособен на технических средствах со следующей минимальной конфигурацией, представленной в таблице 1.

Таблица 1 – Состав технических средств

Наименование		**Требования к техническим средствам**	
		ПС Сенсор	**ПС СУС**
Процессор, не хуже		Intel Core, не менее 2 ГГц	
Материнская плата, не хуже		Совместимая с процессорами Intel Core	
Устройство хранения информации:	Интерфейс обмена данными, не хуже	SATA	
	Скорость вращения, не менее, rpm (об/мин)	7200	
	Форм-фактор, не менее	2,5	
	Объём памяти, не менее, Тбайт	1	2
	Контролер RAID5/RAID10	Да	
Объём оперативной памяти, не менее, Гбайт		16	
Сетевое оборудование:	Сетевой адаптер с поддержкой драйверов intel, не менее, 1 Гбит/с	Да	Да
	Сетевой адаптер с поддержкой bypass, не менее, 1 Гбит/с	Да	Нет
	Qlogic Контроллер;	Нет	Да
Порт USB, не хуже		USB 3.0.	
Консоль управления сервером iLOM с KVM и виртуальным CDROM;		Да	

2.2 Программное обеспечение, необходимое для функционирования ПК СОВ

2.2.1 Программное обеспечение ПС Сенсор

1) ПС Сенсор функционирует под управлением операционной системы Astra Linux Special Edition «Смоленск» версии не ниже 1.5.

2) ПС Сенсор для обнаружения сетевых вторжений в контролируемом канале передачи данных сигнатурным методом использует:

– Систему обнаружения атак (СОА) Suricata версии 4.0;

– СОА Bro версии 2.5.2;

– утилиту p0f версии 3.09b.

3) ПС Сенсор использует СОА Bro версии 2.5.2 для обнаружения сетевых вторжений в контролируемом канале передачи данных эвристическим методом обнаружения.

4) ПС Сенсор использует СУБД ClickHouse версии 1.1.54318 для хранения больших данных о событиях информационной безопасности (далее – СИБ), о журналах событий СОА, о событиях аудита безопасности и статистических данных сетевого трафика.

5) ПС Сенсор использует СУБД PostgreSQL версии 9.4 для хранения данных об объектах контролируемой системы, справочных данных, решающих правил сигнатурного анализа (РПСА), чёрных списков, базы уязвимостей.

6) ПС Сенсор использует программу-агент Net-SNMP версии 5.4.3 для мониторинга состояния и работоспособности. Пользователь может включить дополнительное средство мониторинга работоспособности компонентов Zabbix версии 2.2.7, входящее в состав поставки ПК СОВ.

7) ПС Сенсор использует утилиту Afick версии 2.1.3.21.3 для аудита целостности, при котором выявляются несанкционированные изменения объектов ПС Сенсор (ПО, конфигурационных файлов, базы решающих правил сигнатурного анализа, чёрных списков, программных сценариев эвристического анализа).

8) ПС Сенсор использует Mosquitto MQTT broker версии 3.1.1/3.1 для передачи данных и команд между ПС Сенсор и ПС СУС.

2.2.2 Программное обеспечение ПС СУС

1) ПС СУС функционирует под управлением операционной системы Astra Linux Special Edition «Смоленск» версии не ниже 1.5.

2) ПС СУС использует СУБД ClickHouse версии 1.1.54327 для хранения больших данных о событиях информационной безопасности, журналах событий СОА, событиях аудита безопасности и статистических данных сетевого трафика.

3) ПС СУС использует СУБД PostgreSQL версии 9.4 для хранения данных об объектах контролируемой системы, справочных данных, решающих правил сигнатурного анализа, чёрных списков, базы уязвимостей.

4) ПС СУС использует программу-агент Net-SNMP версии 5.4.3 для мониторинга состояния и работоспособности ПС СУС. Пользователь может включить дополнительное средство мониторинга работоспособности компонентов Zabbix версии 2.2.7, входящее в состав поставки ПК СОВ.

5) ПС СУС использует утилиту Afick версии 2.1.3.21.3 для аудита целостности, при котором выявляются несанкционированные изменения объектов ПС СУС (ПО, конфигурационных файлов).

6) ПС СУС использует Mosquitto MQTT broker версии 3.1.1/3.1 для передачи данных и команд между ПС СУС и компонентами, расположенными ниже и выше по иерархии.

7) ПС СУС использует браузер, для выполнения функций ПС СУС, представленных в графическом пользовательском интерфейсе ПС СУС. ПС СУС совместимо со следующими браузерами: Firefox 44.0.2 из состава ОС Astra Linux Special «Смоленск».

2.2.3 Программные библиотеки, необходимые для функционирования ПК СОВ

Для функционирования ПК СОВ необходимы следующие программные библиотеки:

1) beaker версия 1.8.1;
2) clickhouse_driver версия 0.0.8;
3) configparser версия 3.5.0;
4) decorator версия 4.0.11;
5) falcon версия 1.2.0;
6) gostsum;
7) infi.clickhouse_orm версия 0.9.7.post5;
8) iniherit версия 0.3.6;
9) ipaddr версия 2.2.0;
10) jsonschema версия 2.6.0;
11) libc6 версия 2.4 и более поздние;

12) libgost;
13) libparsec-aud2;
14) libparsec-base2;
15) libpdp;
16) lockfile версия 0.12.2;
17) mod_wsgi версия 4.5.15;
18) msgpack_python версия 0.4.8;
19) numpy версия 1.12.1;
20) paho_mqtt версия 1.2.3;
21) pandas версия 0.19.2;
22) parsec-aud;
23) parsec-base;
24) parsec-mac;
25) peewee версия 2.10.1;
26) perl версия 5.14.2-21 и более поздние + deb7u2;
27) perlapi версия 5.14.2;
28) perl-tk;
29) pluton_yoyo версия 5.0.6.fix3.pluton;
30) psutil версия 5.2.2;
31) psycopg2 версия 2.7.1;
32) py_postgresql версия 1.2.1;
33) pygeoip версия 0.3.2;
34) pyinotify версия 0.9.6;
35) python_daemon версия 2.1.2;
36) python_dateutil версия 2.6.0;
37) python_mimeparse версия 1.6.0;
38) python_slugify версия 1.2.4;
39) python версия 3.5;
40) pytz версия 2017.2;
41) requests версия 2.14.2;
42) ruamel.yaml версия 0.15.9;
43) scipy версия 0.19.0;

44) six версия 1.10.0;

45) statsmodels версия 0.8.0;

46) texttable версия 0.8.8;

47) Unidecode версия 0.4.20;

48) valideer версия 0.4.2;

49) leaflet версия 1.2.0;

50) nDPI версия 2.0.0;

51) libhtp версии 0.5.23;

52) bro-af_packet-plugin;

53) qmqtt.

3 ВЫПОЛНЕНИЕ ПРОГРАММЫ

Раздел «Выполнение программы» описан в документе "ПС «СУС-Плутон-М1.0». Руководство оператора", ДБАР.62.01.12.000.182-01 32.

4 СООБЩЕНИЯ ОПЕРАТОРУ

Раздел «Сообщения оператору» описан в документе "ПС «СУС-Плутон-М1.0». Руководство оператора", ДБАР.62.01.12.000.182-01 32.

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

CEF	–	Common Event Format – формат данных, который применяется к данным, поступающим в SIEM-систему
MQTT	–	Message Queue Telemetry Transport –сетевой протокол, работающий поверх TCP/IP, применяемый для взаимодействия между устройствами (machine-to-machine)
SIEM	–	Security information and event management – класс ПО, который обеспечивает собор в одном месте событий, генерируемых различными системами информационной безопасности и корреляционный анализ событий в реальном времени
АБ	–	Администратор безопасности
БД	–	База данных
БКЦ	–	База контроля целостности
ГПИ	–	графический пользовательский интерфейс
КА	–	Компьютерные атаки
НЖМД	–	Накопитель на жёстких магнитных дисках
ОВК	–	Оператор визуального контроля
ОЗУ	–	Оперативное запоминающее устройство, оперативная память
ОС	–	Операционная система
ПК	–	Программный комплекс
ПС	–	Программное средство
СИБ	–	События информационной безопасности
СОА	–	Система обнаружения атак
СОВ	–	Система обнаружения вторжений
СУБД	–	Система управления базами данных
СУС	–	Сервер управления сенсорами
ЦПУ	–	Центральное процессорное устройство

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

Изм.	Номера листов (страниц)				Всего листов (стр.) в документе	Номер документа	Входящий номер сопроводительного документа	Подпись	Дата
	изме-ненных	заменен-ных	новых	аннулиро-ванных					