Система регистрации, анализа и мониторинга событий информационной безопасности

Система регистрации, анализа и мониторинга событий информационной безопасности (Система РАМС ИБ) представляет собой многоуровневую информационно-аналитическую систему, используемую для обеспечения постоянной защищенности автоматизированных информационных систем (АИС) как небольших организаций, так и распределенных систем федерального масштаба. Отличительной особенностью Системы РАМС ИБ является возможность контроля изолированных АРМ и локальных сетей, не включённых в корпоративные информационные системы.

Под событиями информационной безопасности (СИБ) в АИС подразумеваются любые непредвиденные или нежелательные события, которые нарушают (или могут нарушить) требования информационной безопасности, а именно:

- **несанкционированное уничтожение и изменение информации;**
- **несанкционированное блокирование средств, обеспечивающих доступ к информации;**
- **создание нештатных режимов работы программных (программно-аппаратных) средств за счет преднамеренных изменений служебных данных и настроек;**
- **несанкционированное копирование и распространение информации.**

Система РАМС ИБ способна регистрировать следующие СИБ:

- **несоблюдение требований (политик) по обеспечению ИБ при работе пользователей в АИС;**
- **несанкционированное использование вычислительных ресурсов АИС;**
- **нарушение правил доступа к объектам операционных систем (папки и файлы файловой системы, ключи реестра, запуск процессов, попытки записи информации на незарегистрированные флеш-диски и т.п.);**
- **обнаружение компьютерных атак (КА) на вычислительные ресурсы АИС методами сигнатурного и поведенческого анализа, включая КА следующих типов: «отказ в обслуживании» (DoS), «распределённый отказ в обслуживании» (DDoS), «активность бот-сетей»;**
- **перегрузка вычислительных ресурсов АИС, приводящая к невозможности функционирования заданных сервисов.**

Источниками информации в Системе РАМС ИБ являются:

- **аппаратно-программные комплексы обнаружения компьютерных атак «Аргус»;**
- **хостовые агенты мониторинга параметров объектов операционной системы Microsoft Windows, которые устанавливаются на хостах - АРМах (в том числе изолированных от сети) и серверах, требующих мониторинга;**
- **анализаторы текстовых журналов аудита и сообщений BSD syslog, обеспечивающие получение и анализ информации из указанных источников по настраиваемым алгоритмам анализа.**

Основные функции и особенности хостового агента:

- **удаленное получение и обновление политик информационной безопасности, контролируемых агентом;**
- **контроль / принуждение к исполнению установленной политики информационной безопасности;**
- **шифрование трафика;**
- **синхронизация времени агента с временем управляющего сервера;**
- **надежное скрытие всех элементов агента (файлов, используемых ключей системного реестра, сетевых соединений, процесса);**
- **возможность запуска приложений по расписанию;**
- **удалённая визуализация и управление состоянием модулей агента (загрузка, выгрузка, запуск, останов, смена текущей активной версии модуля);**
- **передача/получение сообщений через альтернативные маршруты (альтернативные транспортные серверы);**
- **возможность немедленной реакции на заданные СИБ;**
- **функционирование под управлением ОС Windows 32 и 64 разряда: XP/2003 Server/ Vista/ 7/2008 Server / 8/ 8.1/2012 Server.**

Схема взаимодействия компонентов Системы РАМС ИБ приведена ниже.

Встроенная в Систему РАМС ИБ аналитическая отчётная система является удобным инструментом администраторов безопасности для эффективного расследования инцидентов ИБ, а также для предоставления статистики событий в АИС по различным параметрам: ID анализатора, IP адрес источника сообщения, IP адрес приемника, порт источника, порт приемника, протокол, важность / критичность сообщения, сработавшая сигнатура,

произошедшее СИБ, временной интервал и др. В случае необходимости, возможно использование внешних систем мониторинга, например HP ArcSight.

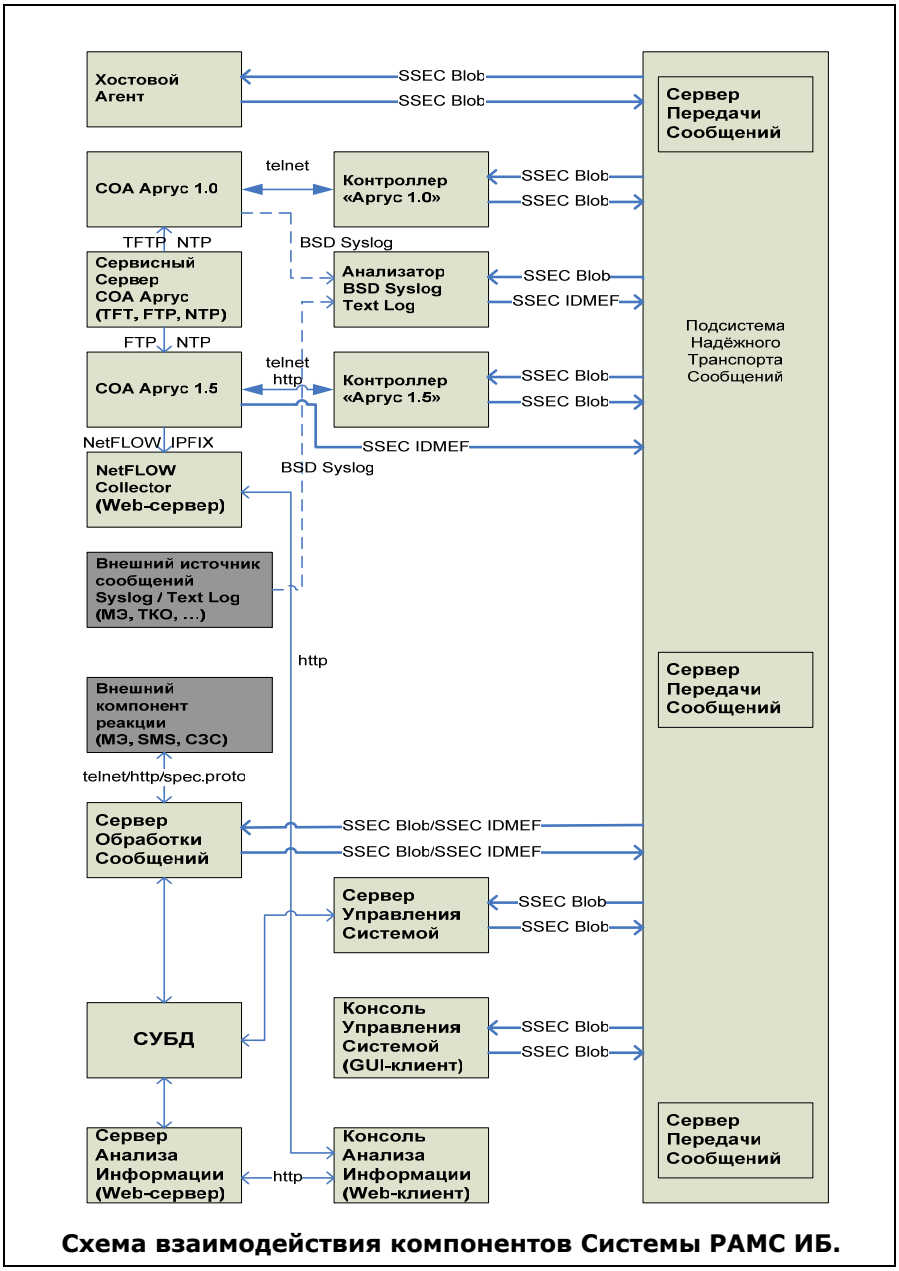

Схема взаимодействия компонентов Системы РАМС ИБ.

Система РАМС ИБ имеет возможность управления:

- **Модулями реакции хостовых агентов, которые могут:**
  а) прекращать выполнение заданных процессов в операционной системе (ОС);
  б) прерывать текущую сессию пользователя ОС, блокировать учётную запись пользователя;
  в) устанавливать фильтры, блокирующие:
  - ✓ **доступ к объектам файловой системы и системного реестра;**
  - ✓ **сетевые взаимодействия;**
  - ✓ **запуск процессов;**
  - ✓ **подключение USB-устройств к компьютеру.**
- **Внешними межсетевыми экранами посредством установки фильтров, блокирующих сетевые взаимодействия.**

Использование системы РАМС ИБ эффективно:

- **при разработке и применении технических мер защиты информации в ИСПДн, предоставляющих информационные услуги удаленным пользователям, в частности в рамках построения порталов госуслуг;**
- **при разработке и применении технических мер защиты информации в территориально распределенных системах, в том числе имеющих изолированные АРМы и сегменты.**