# Аппаратно-программный комплекс обнаружения компьютерных атак «Аргус» версии 1.5

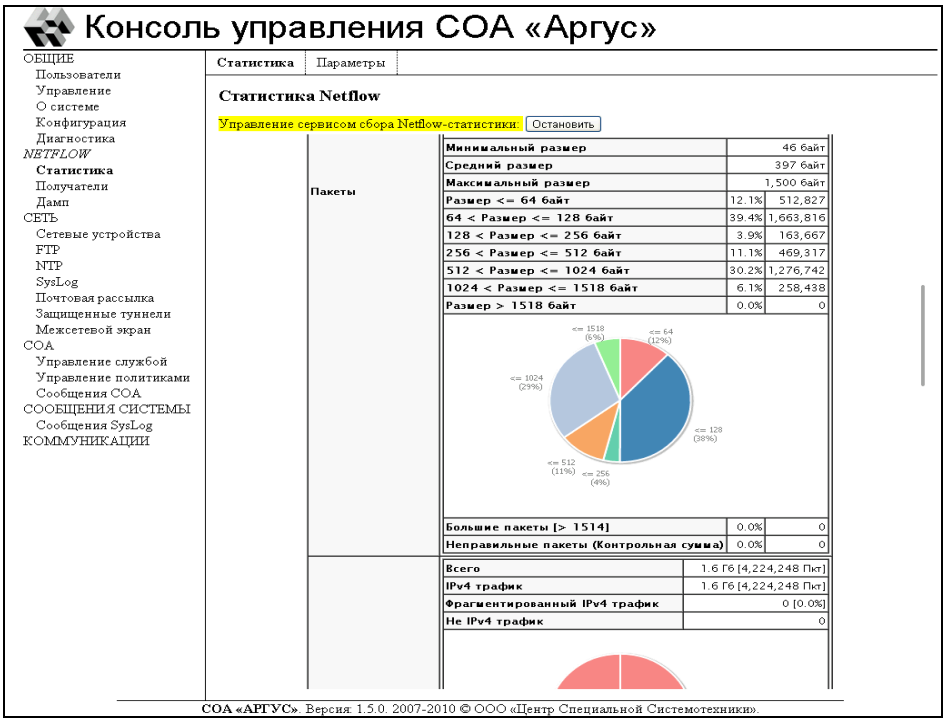
**Аппаратно-программный комплекс обнаружения компьютерных атак "Аргус" (АПК Аргус) версии 1.5 предназначен для обнаружения вторжений и подозрительных воздействий, которые могут нанести вред наиболее критичным компонентам автоматизированных информационных систем (АИС): операционным системам, приложениям, реализующим сетевые сервисы информационных систем, а также хранящейся и обрабатываемой в сети информации. Совместно с другим продуктом компании ООО «Центр специальной системотехники» - Системой РАМС ИБ данный комплекс обеспечивает надежное предотвращение вторжений на скорости канала до 1 Гбит/сек в каждом из направлений передачи данных (при подключении к линии в режиме Full-Duplex).**

**АПК Аргус может использоваться в АИС, обрабатывающих конфиденциальную информацию органов государственной власти Российской Федерации, органов государственного управления и других организаций Российской Федерации, а также может использоваться для создания автоматизированных систем класса защищенности до 1Г включительно и для защиты информации в информационных системах персональных данных до 1 класса включительно.**

**Для обнаружения компьютерных атак АПК Аргус версии 1.5 выполняет сигнатурный анализ сетевого трафика, анализ протоколов, анализ аномалий по накопленной статистике для протоколов 3-7 уровней эталонной модели взаимодействия открытых систем (ЭМВОС).**

**АПК Аргус версии 1.5 имеет встроенные пользовательские интерфейсы для анализа событий ИБ, подготовки отчетов операторами и администраторами комплекса.**

**Комплекс дает возможность получения широкого набора статистических данных в виде диаграмм и таблиц, которые доступны для анализа через Web-интерфейс. Копия экрана консоли управления с одним из примеров представлена ниже:**




**Пример отчета Netflow-статистики, доступного через Web-интерфейс.**

**В комплекс включены наборы отчетов по Netflow-статистике для анализа следующих данных:**

- **хосты, использующие большой процент пропускной способности сети;**
- **хосты с большим числом контактов с другими хостам сети;**
- **хосты, использующие запрещенные протоколы или некорректно использующие разрешенные протоколы;**
- **общее процентное соотношение используемых протоколов, в том числе и соотношение трафика протоколов TCP и UDP;**

- **общие показатели трафика: количество пакетов, объем;**
- **общее распределение трафика по портам TCP и UDP;**
- **список активных хостов в сети с индивидуальными общими характеристиками трафика хостов (размер, пакеты, используемые протоколы, TCP/UDP-сессии и TCP/UDP-порты);**
- **загруженность сети по задаваемым интервалам времени;**
- **общее процентное соотношение трафика между хостами локальной подсети и между локальными и внешними хостами;**
- **матрица хостов локальной сети с объемом трафика, которым они обмениваются.**

**На основе перечисленных данных можно обнаруживать DoS / DDoS атаки, сканирование хостов и другие аномалии сетевых взаимодействий в информационной системе, а также устанавливать хосты, входящие в бот-сети.**

**Для достижения наибольшей гибкости и точности настройки Комплекса используется язык интерпретируемых сценариев. Механизм сценариев предназначен для задания логики и образцов искомых в трафике данных, а также для задания правил корреляции зарегистрированных событий.**

**Отдельно можно выделить возможности объекта сигнатуры, инкапсулирующего входные данные для сигнатурного анализа:**

- **устанавливать зависимости между сигнатурами в рамках соединения (например, условием проверки текущей сигнатуры является срабатывание другой сигнатуры, настроенной на ответ сервера об ошибке);**
- **задавать несколько регулярных выражений;**
- **задавать регулярные выражения только для заголовка или тела пакета;**
- **вследствие того, что объект имеет доступ к контексту соединения для прикладных протоколов, можно параметризировать свойства соединения, в рамках которого ожидается реакция: направление, статус, порт, адрес, протокол.**

**С помощью сценариев можно получать доступ к данным анализаторов протоколов АПК Аргус версии 1.5 и описывать, что следует предпринять в обработчике событий. Обработчики событий могут управлять и обновлять информацию об общем состоянии системы, генерировать новые события, запускать функции, генерировать уведомления с сигналами тревоги и направлять их внешним получателям по e-mail. Механизмы настройки сценариев позволяют сократить: ручное редактирование, число вносимых ошибок и время настройки Комплекса.**

**Сценарии и сигнатуры поставляются ООО «ЦСС», а также могут перенастраиваться и разрабатываться администраторами безопасности конкретных организаций. Через механизм сценариев можно настраивать поддерживаемые в настоящее время анализаторы протоколов Комплекса:**

- **транспортного уровня: ARP, IP, ICMP, TCP, UDP;**
- **прикладного уровня: DHCP, SunRPC, DCE_RPC, DNS, Finger, Gnutella, FTP, HTTP, Ident, IRC, Netbios-SSN, NCP, NFS, NTP, POP3, Portmapper, RSH, Rlogin, SMB, SSH, SSL, SMTP, Telnet.**

**На основе сценариев можно организовать политики безопасности, которые будут предназначены для контроля трафика на предмет наличия:**

- **активности бот-сетей;**
- **вирусной активности;**
- **разведки IT-ресурсов (сетевое сканирование);**
- **использования сетевых приложений (Web, ICQ и т.д.);**
- **атак типа Bruteforce (перебор паролей методом «грубой силы») для протоколов HTTP, FTP, SMB, SSH, Telnet и др.;**
- **инкапсуляции протоколов с целью создания туннелей;**
- **аномалий в работе протоколов и отклонений от RFC на основе статистического и эвристического анализа;**
- **распределенных во времени атак, проводимых с использованием различных протоколов.**

**Таким образом, применение АПК Аргус высокоэффективно в качестве средства обнаружения и расследования инцидентов, выявления небезопасных служб и участков сети организации, а также в определении производительности сети.**

**АПК Аргус соответствует требованиям ФСБ России к системам обнаружения компьютерных атак класса В – регистрационный номер Сертификата соответствия СФ/СЗИ-0039 от "25" декабря 2014 г. (срок действия – до 31 декабря 2017 г.), а также имеет Сертификат соответствия ФСТЭК России № 2487 от 23 ноября 2011 г. (срок действия – до 23 ноября 2017 г.).**