МЕХАНИЗМЫ ОПЕРАЦИОННЫХ СИСТЕМ ASTRA LINUX ДЛЯ КОНТРОЛЯ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ СЕТЕЙ

С.И. Павлович

Под безопасностью информационных сетей следует понимать такое их состояние, при котором они защищены от внутренних и внешних угроз, направленных на нарушение свойств конфиденциальности, целостности и/или доступности циркулирующей в рамках них информации. В связи с этим контроль безопасности информационных сетей заключается в периодической реализации оценки указанных свойств их объектов. Такая оценка может проводиться как с помощью специального программного обеспечения, так и с помощью тех механизмов, которые включены в состав используемых в рамках информационных сетей операционных систем. Автором выполнен анализ механизмов операционных систем специального назначения Astra Linux, которые могут быть использованы для контроля безопасности информационных сетей, в рамках которых используются эти системы. Определено, что к таким механизмам относятся следующие.

1. Средства контроля целостности, в частности:

- подсчета контрольных сумм;

- контроля соответствия дистрибутиву;
- регламентного контроля целостности;
- средства проверки электронной подписи.

2. Фильтрация сетевого потока.

3. Контроль подключения съемных носителей.

4. Средства управления протоколированием, в частности:

- утилита fly-admin-viewaudit, применяемая для выборочного просмотра журналов аудита;
- команда getfaud, применяемая для получения информации о правилах протоколирования, реализуемых в отношении файловых объектов;
- команда useraud, применяемая для получения информации о правилах протоколирования, реализуемых в отношении действий пользователей;
- команда psaud, применяемая для получения информации о правилах протоколирования, реализуемых в отношении какого-либо выбранного процесса;
- команда parselog, применяемая для анализа двоичных файлов аудита, записанных с помощью parlogd;
- команды kernlog и userlog, применяемые для анализа двоичных файлов регистрации событий, связанных с функционированием ядра операционной системы и действиями пользователей соответственно;

5. Средства централизованного аудита и протоколирования.

Механизмы, представленные в пп. 1–3, могут быть отнесены к механизмам, реализуемым операционной системой, а механизмы, представленные в пп. 4, 5 – к механизмам, используемым администратором информационной сети.