**АВТОМАТИЗАЦИЯ УПРАВЛЕНИЯ ДОСТУПОМ К РЕСУРСАМ ОС ASTRA LINUX SE**

В настоящее время активно идет процесс внедрения в деятельность органов государственной охраны информационных систем на базе ОС Astra Linux. Кроме того, ОС Astra Linux внедряется и в учебный процесс академии. Одной из задач, которая постоянно возникает в ходе эксплуатации распределенных компьютерных сетей и систем как в практических подразделениях, так и в ходе учебного процесса, является контроль и управление доступом к ресурсам этих сетей и систем. В этой связи были определены следующие требования к администрированию ОС Astra Linux:

– способность выполнять такие задачи как управление пользователями и группами, управление политиками безопасности, настройка удаленного доступа к файлам, монтирование файловых систем;

– возможность удаленного администрирования серверов и рабочих станций, т.е. выполнения задач администрирования, не имея физического доступа к оборудованию;

– возможность выполнять мониторинг состояния серверов и рабочих станций, а также действий пользователя;

– возможность контролировать и применять политики управления доступом к ресурсам к целым группам однотипных серверов и рабочих станций (например, ко всем рабочим станциям учебного компьютерного класса).

Для выполнения первого требования в ОС Astra Linux имеется большой набор системных утилит :

– для управления пользователями и группами используются консольные утилиты useradd, usermod, userdel, groupadd, groupmod, groupdel;

– для управления политиками безопасности используются консольные утилиты chmod, chown, а так же модуль «Киоск» в ОС Astra Linux;

– настройка удаленного доступа к файлам состоит в настройке файлового сервера Samba при помощи текстового конфигурационного файла smb.conf;

– задача монтирования файловых систем решается при помощи утилиты mount и изменения файла fstab.

Для решения задач удаленного администрирования разработаны необходимые сетевые протоколы и программное обеспечение. Программы удалённого администрирования **–** программы или функции операционных систем, позволяющие получить удалённый доступ к компьютеру через локальные или глобальные сети и выполнять на них функции администрирования в реальном времени. По типу интерфейса эти программы можно разделить на программы с консольным и визуальным интерфейсом. Одними из самых популярных и распространённых программ являются: PuTTy, TeamViewer, Mikogo, и др.

Для передачи команд администрирования и вывода экрана используются протоколы удалённого администрирования: RDP, RFB, Telnet, Rlogin, и собственные. Для шифрования трафика в программах удалённого администрирования используются протоколы SSH, SSL, TLS и другие. Протоколы RDP, RFB, X11 являются протоколами удаленного доступа к рабочему столу компьютера. Протоколы Telnet, Rlogin используются для передачи текстовых команд командных оболочек.

В операционных системах на базе Unix чаще всего применяется протокол SSH ввиду своей универсальности и безопасности. SSH – это сетевой протокол прикладного уровня, позволяющий производить удалённое управление операционной системой и туннелирование соединений транспортного уровня. SSH шифрует весь телетрафик, включая передаваемые пароли. При этом допускается выбор алгоритмов шифрования.

Основной реализацией данного протокола в Unix-подобных системах является пакет OpenSSH. Он содержит:

– ssh-клиент;

– демон sshd, реализующий функции ssh-сервера и SFTP-сервера;

– модуль генерации ключей;

– утилиту для проверки ключей хостов.

Сервер OpenSSH может аутентифицировать пользователей, используя встроенные механизмы аутентификации, такие как публичные ключи, клавиатурный ввод (пароли и запрос-ответ), Kerberos/GSS-API.

Наиболее предпочтительным для решения поставленных задач администрирования является применение метода аутентификации на основе публичных ключей. Это позволяет подключаться к администрируемым машинам без ввода парольной фразы. Но это требует предварительной настройки администрируемого компьютера.

Для решения задач группового администрирования в ОС Astra Linux в настоящее время нет встроенных программных средств. Была разработана архитектура распределенной системы контроля и управления доступом к ресурсам ОС. Она включает в себя следующие компоненты:

**Управляющий сервер** – сервер, осуществляющий аутентификацию подключаемых к нему компьютеров, мониторинг состояния машин, генерацию исполняемых скриптов, добавление задач на выполнение, отсылку скриптов администрируемым компьютерам и контроль за правильностью их выполнения. Для генерации скриптов используется программа, написанная на языке Python. В качестве планировщика задач используется демон Cron. Для удаленного выполнения скриптов используется OpenSSH-клиент.

**База данных** хранит в себе данные пользователей, имеющих доступ к системе администрирования, набор базовых шаблонов настроек, список заданий для настройки.

**Шаблоны настроек –** базовый скрипт или набор скриптов для выполнения определенных административных задач, таких как управление пользователями, настройка веб-сервера, управление устройствами, настройка политик безопасности и т. д.

**Веб-интерфейс** предоставляет доступ пользователям к системе администрирования и выполняет следующие функции:

– добавление шаблонов для настроек администратором;

– регистрация новых пользователей администратором;

– подача заявок на настройки пользователями.

**Администратор** осуществляет формирование шаблонов для различных задач администрирования, регистрирует новых пользователей, осуществляет контроль за работой системы, а также принимает решения по поводу заявок на удаленную настройку.

В рамках научной работы был создан макет данной системы. В себя он включает модуль мониторинга состояния, планировщик, модуль генерации скриптов.

Также, была разработана методика настройки администрируемых машин.