В связи с тенденцией перехода на свободное программное обеспечение

в деятельность органов государственной охраны активно внедряются различные программные продукты с открытым исходным кодом. Одним из таких продуктов является операционная система Astra Linux Special Edition. Она предназначена для создания на ее основе автоматизированных систем в защищенном исполнении, обрабатывающих информацию со степенью секретности "совершенно секретно" включительно. На ее основе возможно, как создание отдельных объектов ЭВТ, так и развертывание распределенных локальных вычислительных систем.

Для обеспечения эффективного и безопасного функционирования ИС на базе Astra Linux требуется обеспечить качественную настройку и конфигурирование программного обеспечения и самой операционной системы. Данные задачи решаются в процессе системного администрирования.

В процессе администрирования компьютерных сетей иногда возникают задачи выполнения большого количества однотипных операций на некотором числе машин. Например, установка, обновление, удаление программного обеспечения; управление пользователями; управление доступом к логическим томам, сетевым хранилищам, съемным носителям. При этом, в сеть может быть объединено большое количество машин.

Решать эти задачи можно разными способами. Первый – это вручную применять требуемые настройки на каждой машине. Данный способ можно применять при небольшом числе компьютеров в сети, но он имеет следующие существенные недостатки:

1. Для применения какого-либо набора требуемых изменений на большом количестве машин требуется большое количество времени, что в некоторых случаях является критичным;
2. Невозможно осуществить оперативный контроль применения набора конфигураций при большом числе машин;
3. Возможность совершения ошибок администратором.

Также, необходимо учитывать, насколько сильно вычислительная сеть распределена. Разнесение узлов на большие расстояния значительно уменьшает оперативность выполнения необходимых задач. Для устранения данного недостатка администрирование удаленных узлов осуществляю удаленно при помощи специального программного обеспечения. Основными являются программы получения доступа к удаленной командной строке и удаленному рабочему столу.

Несмотря на устранение данного недостатка, метод удаленного администрирования так же не дает возможность быстрого применения необходимых конфигураций на большом количестве машин; не позволяет осуществить оперативный контроль применения набора конфигураций; не защищает от возможных ошибок администратора. Для того, чтобы устранить первые два недостатка можно автоматизировать процесс применения конфигурации и контроля результата изменения состояния системы. Возможно применения планировщиков, написание специальных скриптов, которые бы осуществляли групповое применения необходимых изменений или применение готовых программных продуктов, автоматизирующие эти задачи. Для уменьшения числа ошибок необходимо заранее определить исходное состояние машин; установить, что необходимо сделать, для применения требуемых конфигураций; сформировать готовые шаблоны, скрипты; желательно, задокументировать набор применяемых изменений в системе; и обязательно осуществлять контроль за результатом применения конфигурации.

Описанные пути устранения недостатков представляют собой процессы, которые включает в себя управление конфигурациями.

Управление конфигурациями - в системной инженерии, это процесс установления и поддержания постоянства качества продукта, функциональных и физических свойств в соответствии с их требованиями, архитектурных и эксплуатационных сведений на всех жизненном цикле. Управление конфигурациями, рассматривая приложение к жизненному циклу систем, обеспечивает представление и контроль за их производительностью, функциональными и физическими атрибутами. Управление конфигурацией обеспечивает подтверждение того, что система работает как задумано, и определена и задокументирована достаточно детально для поддержки этого проекта на протяжении жизненного цикла. Управление конфигурациями облегчает связь управления информацией о системе и системными изменения для таких полезных целей, как пересмотр возможностей, повышение производительности, надежности или ремонтопригодности, увеличение срока службы, уменьшение стоимости, уменьшение риска и помех или дефектов.

Управление конфигурациями подчеркивает функциональную связь между частями, подсистемами и системами для эффективного контроля системных изменений. Это помогает убедиться в том, что предложенные изменения систематически проверены для минимизации неблагоприятных эффектов. Изменения в системе предложены, оценены и реализованы с использованием стандартизированного, системного подхода, который обеспечивает согласованность, и предлагаемые изменения оцениваются с точки зрения их ожидаемого воздействия на всю систему. Управление конфигурациями обеспечивает проверку того, что изменения проводятся в соответствии с предписаниями и что документация элементов и систем отражает их истинную конфигурацию. Полная программа управления конфигурацией включает в себя положения для хранения, отслеживания и обновления всей системной информации о компонентах, подсистемах и системной основе. Структурированная программа управления конфигурациями гарантирует, что документация на элементы составлена правильно и согласована с актуальной физической архитектурой элемента.

Управление конфигурациями это практика систематического управления конфигурациями так, что система сохраняет целостность на протяжении времени. Управление конфигурациями внедряет политики, процедуры и инструменты, которые необходимы для управления, оценки предложенных изменений, отслеживания состояния изменения и составление описи системы, и поддержка документирования системных изменений. Управление конфигурациями составляет программу и план обеспечения технического и административного руководства разработкой и внедрением процедур, функций, служб, инструментов, процессов и ресурсов, необходимых для успешной разработки и поддержки сложных систем. В течение разработки системы, управление конфигурацией позволяет управлять программой для отслеживания требований на протяжении всего жизненного цикла путем принятия и эксплуатации и технического обслуживания. Как изменения неизбежны из требований и дизайна, они должны быть утверждены и документированы, создавая точный отчет о состоянии системы. В идеале процесс управления конфигурациями применяется на протяжении всего жизненного цикла системы.

Процесс управления конфигурациями описан в большом количестве стандартов. В Российской Федерации данный процесс определен в стандарте ГОСТ Р ИСО 10007-2007. В этом стандарте описаны пять процессов, которые выполняются в качестве политик и процедур для определения базовых конфигураций, и выполнения стандартного процесса управления изменениями.

Управление конфигурациями состоит из следующих процессов:

* Планирование управления конфигурацией
* Идентификация конфигураций
* Управление изменениями
* Учет статуса конфигураций
* Аудит конфигурации

Управление конфигурацией используется для поддержания понимания статуса сложных активов с целью поддержания высокого уровня удобства эксплуатации при самой низкой стоимости. В частности, она направлена на обеспечение того, что деятельность системы не нарушается из-за превышения предела планируемого срока службы или снижения уровня качества этих активов (или части активов).

Применительно к операционным системам, управление конфигурациями обеспечивает идентификацию начального состояния системы; контроль применения конфигураций (ограничения числа лиц, допущенных к управлению или числа программ и служб, которые доступны для конфигурирования); учет статуса конфигурации; отслеживание конфигураций и аудит примененных конфигураций. Данный процесс обеспечивает специализированное ПО, позволяющее автоматизировать этапы управления конфигурацией.

Система управления конфигурацией - это программный комплекс, обеспечивающий автоматизацию планирования, изменения, контроля и учета состояния конфигураций рабочих станций и серверов. Часто, в зависимости от масштабов системы УК, она может не включать некоторые функции процесса УК, перенося ответственность их выполнения на администратора.

В контексте информационной безопасности процесс Управления конфигурациями имеет наибольшее значение, так как он позволяет классифицировать Конфигурационные Единицы, то есть определить информационные активы и установить их критичность. Эта классификация определяет связи между Конфигурационными Единицами и предпринимаемыми мерами или процедурами безопасности.

Классификация Конфигурационных Единиц определяет их конфиденциальность, целостность и доступность. Каждая Конфигурационная Единица в Конфигурационной Базе Данных должна быть классифицирована. Эта классификация связывает Конфигурационную Единицу с соответствующим комплексом мер безопасности или процедурой.

Виды работ, выполняемых в рамках Процесса Управления Изменениями, часто бывают тесно связаны с безопасностью, так как управление изменениями и управление информационной безопасностью взаимозависимы. Если достигнут приемлемый уровень безопасности, который находится под контролем процесса управления изменениями, то можно гарантировать, что этот уровень безопасности будет обеспечиваться и после проведения изменении. Для поддержки этого уровня безопасности существует ряд стандартных операций. Каждый Запрос на изменения связан с рядом параметров, которые определяют процедуру приемки. Параметры срочности и степени воздействия могут быть дополнены параметром, связанным с безопасностью. Если Запрос на изменения может оказать значительное воздействие на информационную безопасность, потребуются расширенные приемочные испытания и процедуры.

Любые меры безопасности, связанные со внесением изменений, должны реализовываться одновременно с проведением самих изменений, и они должны тестироваться совместно. Тесты безопасности отличаются от обычных функциональных тестов. Задачей обычных тестов является определение доступности определенных функций. При тестировании безопасности проверяют не только доступность функций безопасности, но также отсутствие других, нежелательных функций, которые могут снизить безопасность системы.

С точки зрения безопасности управление изменениями является одним из наиболее важных процессов. Это объясняется тем, что Управление Изменениями вводит новые меры безопасности в ИТ-инфраструктуру вместе с изменениями этой инфраструктуры.

В настоящий момент, в составе Astra Linux не имеется системы управления конфигурациями. Процесс управления конфигурацией в вычислительных сетях, состоящих машин под управлением данной ОС осуществляется вручную локально или удаленно. Отсюда выходят следующие недостатки:

1. Для применения какого-либо набора требуемых изменений на большом количестве машин требуется большое количество времени, что в некоторых случаях является критичным;
2. Невозможно осуществить оперативный контроль применения набора конфигураций при большом числе машин
3. Возможность совершения ошибок администратором.

Из вышесказанного можно вывести следующие цели создания системы УК для ОС Astra Linux:

* Повышение оперативности процесса управления конфигурацией серверов и рабочих станций;
* Автоматизация процесса контроля конфигураций серверов и рабочих станций.

В процессе создания системы необходимо провести сравнение уже имеющихся программных продуктов, выделить наиболее подходящие, исходя из предъявляемых требований, определить каким образом требуется модифицировать данные решения для того, чтобы оно отвечало требованиям.

Ограничения для системы УК:

1. На рабочих станциях и серверах применяется Astra Linux;
2. Управление конфигурацией должно осуществляться удаленно;
3. Для осуществления требуемых изменений необходимо знать административный пароль.

Требования к разрабатываемой системе определяются критериями оперативности, результативности и ресурсоемкости.

Сформулируем критерий оперативности.

Пусть – множество требуемых наборов конфигураций, – некоторый набор конфигураций, входящий в множество требуемых конфигураций.  *-* функция применения набора конфигураций на множестве машин.

Критерий оптимальности определяется тем, что время применения набора конфигурации не превышает некоторое допустимое время, т. е.:

Так как процесс применения конфигурации на целевых машинах является случайным процессом, то критерий оперативности преобразуется к следующему виду:

Вероятность того, что время применения набора конфигураций не превысит допустимое время, не меньше некоторого значения.

При рассмотрении применения данной системы в учебном процессе Академии допустимое время определяется длительностью перерыва между учебными занятиями, в течение которого возможно изменение конфигурации. Вероятность = 0.9.

Критерий результативности определяется как отношения числа успешно примененных наборов конфигураций к общему числу наборов.

Исходя из раннее описанных ограничений определим требования к системе УК:

* Возможность удаленного управления целевыми машинами
* Возможность группового применения конфигураций
* Осуществление контроля за результатом применения конфигурации
* Возможность изменения конфигурации в соответствии с некоторым планом, расписанием
* Наличие удобно интерфейса администрирования