МЕЖГОСУДАРСТВЕННОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ОБРАЗОВАНИЯ
«БЕЛОРУССКО-РОССИЙСКИЙ УНИВЕРСИТЕТ»

Кафедра «Автоматизированные системы управления»

ИННОВАЦИОННЫЕ ТЕХНОЛОГИИ ОБЕСПЕЧЕНИЯ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ

Методические рекомендации к лабораторным работам для студентов специальности 1-40 80 02 «Системный анализ, управление и обработка информации» дневной и заочной форм обучения

Могилев 2020

УДК 004.4
ББК 32.973.202
И66

Рекомендовано к изданию
учебно-методическим отделом
Белорусско-Российского университета

Одобрено кафедрой «Автоматизированные системы управления» «09» июня 2020 г., протокол № 11

Составители: д-р техн. наук А. И. Якимов;
ст. преподаватель Е. А. Зайченко;
М. Н. Пранович

Рецензент Ю. С. Романович

Изложены указания к выполнению лабораторных работ по дисциплине «Инновационные технологии обеспечения компьютерной безопасности системы». Приведен перечень необходимой литературы.

Учебно-методическое издание

ИННОВАЦИОННЫЕ ТЕХНОЛОГИИ ОБЕСПЕЧЕНИЯ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ

Ответственный за выпуск А. И. Якимов

Корректор Т. А. Рыжикова

Компьютерная верстка Е. В. Ковалевская

Подписано в печать 16.10.2020 . Формат 60 × 84/16. Бумага офсетная. Гарнитура Таймс. Печать трафаретная. Усл. печ. л. 1,4 . Уч.-изд. л. 1,31 . Тираж 16 экз. Заказ № 564.

Издатель и полиграфическое исполнение:
Межгосударственное образовательное учреждение высшего образования
«Белорусско-Российский университет».
Свидетельство о государственной регистрации издателя,
изготовителя, распространителя печатных изданий
№ 1/156 от 07.03.2019.
Пр-т Мира, 43, 212022, Могилев.

Содержание

Введение

Цель учебной дисциплины состоит в формировании у магистранта знаний, умений, навыков, необходимых при использовании инновационных технологий обеспечения безопасности для автоматизированных систем обработки информации.

В результате изучения дисциплины магистрант узнает:

– основные модели построения защищенных автоматизированных систем;

– современные подходы к построению систем защиты информации;

– методы концептуального проектирования технологий обеспечения информационной безопасности.

Одной из наиболее эффективных форм получения знаний является выполнение лабораторных работ. В методических рекомендациях содержатся:

– теоретические сведения к лабораторным работам;

– условия задач для самостоятельного выполнения;

– список рекомендуемой литературы.

Общие требования к отчету

Отчет должен содержать стандартные составные части.

1 Титульный лист с указанием следующих реквизитов: название учреждения образования, название закрепленной за дисциплиной кафедры, номер и название лабораторной работы, название дисциплины, вариант, ФИО и группа выполнившего лабораторную работу, должность и ФИО проверяющего работу, место и дата составления отчета.

2 Цель работы.

3 Постановка задачи.

4 Полный перечень использованных команд с кратким описанием их назначения.

5 Примеры выполнения команд, которые были использованы в ходе работы с описанием результатов их выполнения.

6 Выводы по теме лабораторной работы.

Отчет оформляется шрифтом гарнитуры TimesNewRoman, кегль – 14, междустрочный интервал – полуторный, абзацный отступ – 1,25 см.

Страницы должны быть пронумерованы вверху посередине. Титульный лист при нумерации считается, но не нумеруется.

Лабораторная работа № 1. Работа с учётными записями пользователей и группами

Цель работы: изучить особенности и освоить навыки администрирования локальных учётных записей пользователей и групп в операционных системах специального назначения (ОССН) с использованием командной строки и графического интерфейса.

Общие положения

ОССН – многопользовательская ОС, потому учётная запись пользователя – ключевой элемент всей системы управлении доступом. Для идентификации учётных записей пользователей и групп в ОССН, как во всех ОС семейства Linux, используются *uid* и *gid* соответственно. Каждый пользователь должен принадлежать как минимум к одной группе – первичной группе. При создании учётной записи польэователя командой *adduser* или с использованием графической утилиты *fly-admin-smc* создаётся группа, имя которой совпадает с системным именем учётной записи пользователи. Данная группа применяется как первичная группа и будет задана идентификатором в учётной записи пользователя, расположенной в файле */etc/passwd*. Учётная запись пользователя может входить более чем в одну группу.

Для администрирования параметров учётных записей пользователей используются следующие команды и утилиты:

– *useradd* и *adduser* – команды добавления учётной записи пользователя;

– *passwd* – команда смены пароли учётной записи пользователя;

– *usermod* – команда модификации параметров уже существующей учётной записи;

– *userdel* – команда удаления учётной записи пользователя;

– *gpasswd* – команда управления группами;

– *addgroup* – команда создания группы;

– *delgroup* – команда удаления группы;

– *fly-admin-smc* – графическая утилита, позволяющая решать комплекс задач по администрированию учётных записей пользователей и групп, в том числе администрировать параметры мандатного управления доступом и мандатного контроля целостности.

Порядок выполнения работы

1 Начать работу со входа в ОССН в графическом режиме с учётной записью пользователя *user* (уровень доступа – 0, неиерархические категории – нет, уровень целостности – «Низкий»).

2 Запустить терминал *Fly*.

3 Определить текущую учётную запись пользователя с использованием команды *whoami*.

4 Проверить наличие права доступа на чтение к файлу */etc/passwd* и получить следующие данные, выполнив команды *cat /etc/*passwd или *less /etc/passwd*:

– количество параметров учётных записей пользователей;

– количество параметров, совпадающих у всех учётных записей пользователей;

– текущее число учётных записей пользователей;

– количество различных используемых командных интерпретаторов.

5 Вывести строку, соответствующую текущей учётной записи пользователя, из файла *etc/pass*wd с использованием команды *cat /etc/passwd | grep "^$(whoami)"*, при этом получить следующие данные:

– наличие пароля или свёртки пароля (вывести эти данные командой *cat /etc/passwd | grep "^$(whoami)" | cut -d : -f2*;

– группа и идентификатор текущей учётной записи пользователя.

6 Добавить две учётные записи пользователей *user1* и *user2* (с соответствующими домашними каталогами) с использованием команд *sudo adduser user1* и *sudo adduscr user2*.

7 Осуществить последовательные попытки входа в ОССН с учётными записями созданных пользователей *user1* и *user2*. При этом осуществить следующие действия:

– проанализировать причины неудачного входа в ОССН с учётной записью пользователя *user1*, сравнив отличия в командах, использованных при модификации параметров учётных записей пользователей *user1* и *user2*;

– вернуть домашний каталог учётной записи пользователя *user1* командой *usermod -u -d /home/user1 user1*, рассмотреть результат её выполнения, проверить запись о домашнем каталоге в файле *etc/passwd*;

– повторно установить домашний каталог пользователя *user1* командой *usermod -ID -d /home/userone user1*, проверить результат;

– проверить *возможность* входа в ОССН с учётной записью пользователя *user1*, выйти из ОССН.

8 Выполнить удаление учётных записей пользователей:

– удалить учётную запись пользователя *user1* с использованием графической утилиты «Управление политикой безопасности»:

– удалить учётную запись пользователя *user2* командой *sudo deluser user2*;

– удалить учётную запись пользователя *user1* командой *sudo userdel user1*:

– проверить наличие домашних каталогов учётных записей пользователей *userl* и *user2,* после чего с использованием справочной информации по команде *userdel* определить её параметры, позволяющие удалить содержимое домашнего каталога учётной записи пользователя;

– удалить домашние каталоги учётных записей пользователей *user1* и *user2* непосредственно командами *rm -s / home/userone* и *rm -s /lunne/usertw*o, осуществив попытки удаления без использования и с использованием команды *sudo*;

– проверить наличие домашних каталогов учётных записей пользователей *user1, user2* в каталоге *home/.pdp*.

Контрольные вопросы

1 Каковы особенности создания учётных записей с использованием команд *adduser*, *useradd* и графической утилиты «Управление политикой безопасности» (*fly-admin-smc*)?

2 Какой группе должна принадлежать учётная запись пользователя, чтобы была возможность выполнения команды *adduser*?

3 Какими командами создаётся учётная запись пользователя и какие дополнительные параметры при этом вводятся?

Лабораторная работа № 2. Создание и настройка параметров мандатного управления доступом и мандатного контроля целостности

Цель работы: изучить и освоить администрирование основных параметров мандатного управления доступом в ОССН с применением графических утилит и консольных команд.

Общие положения

В ОССН, наряду с традиционной для ОС семейства Linux системой дискреционного управления доступом, реализована система мандатного управления доступом и мандатного контроля целостности. С этим связано наличие у сущностей ОССН мандатных меток конфиденциальности и целостности.

Параметрами мандатного управления доступом (мандатной меткой) являются следующие элементы:

– уровень доступа или конфиденциальности (соответствует уровню доступа субъект-сессий или конфиденциальности сущности);

– уровень целостности сущности и субъект-сессии;

– набор неиерархических категорий;

– специальные атрибуты (*CCNR*, *CCNRI*, *EHole*).

При установке ОССН (по умолчанию) задаются следующие параметры мандатного управления доступом и мандатного контроля целостности:

– два уровня целостности («Низкий» – значение 0, «Высокий» – 1);

– четыре уровня доступа/конфиденциальности («Уровень 0» – значение 0, «Уровень 1» – 1, «Уровень 2» – 2, «Уровень 3» – 3);

– неиерархические категории – нет.

Мандатное управление доступом процессов (субъект-сессий) к ресурсам (сущностям) основано на реализации соответствующего механизма в ядре ОС. При этом принятие решения о запрете или разрешении доступа субъект-сессии к сущности осуществляется в соответствии с правилами, описанными в рамках модели, и зависит от запрашиваемого вида доступа (чтение, запись, применение права доступа на выполнение) и мандатного контекста (используемых в запросе уровней конфиденциальности, доступа и целостности).

Практическое задание

1 Начать работу в графическом режиме с учётной записью пользователя *user* (уровень доступа – 0, неиерархические категории – нет, уровень целостности – «Низкий»).

2 Запустить графическую утилиту редактирования учетных записей пользователей «Управление политикой безопасности» через меню «Настройки» главного пользовательского меню.

3 Модифицировать параметры мандатного управления доступом, для этого осуществить следующие действия:

– открыть раздел «Уровни», выбрать «0: Уровень_0)» и переименовать данный уровень доступа: «Уровень 0»;

– осуществить попытку создания уровня доступа с именем «Уровень_4», установив значение, равное 4. Проанализировать результат;

– выполнить создание уровня доступа с именем «Уровень_4», задав значение, равное 1, после чего проверить наличие записи «Уровень_4» в списке «Уровни»;

– выполнить обратное переименование «Уровень 1» в «Уровень 0».

4 Создать учётную запись пользователя *user1*, установив максимальный уровень доступа «Уровень_4».

5 Выполнить удаление уровня доступа 1 из раздела «Уровни» путем выбора в контекстном меню пункта «Удалить».

6 Открыть учётную запись пользователя *user1* и в закладке «Дополнительные» в элементе «Максимальный уровень» проверить наличие записи «(4)», при этом в списке выбора уровня «Уровень 4» будет отсутствовать.

7 Вывести в терминал *Fly* параметры мандатного управления доступом для учётной записи пользователя *user1*. Для этого выполнить следующие действия:

– запустить терминал *Fly* и перейти в каталог */etc/parsec/macdb*;

– прочитать параметры учётной записи *nscil* командой *sudo grep "user1" **;

– определить максимальный уровень доступа учётной записи *user1* командой *sudo grep "user1" * | cat -d : -f 5*;

– определить минимальный уровень доступа учётной записи *user1* командой *sudo grep "user1" * | cat -d : -f* 3 и проверить его соответствие данным, отображаемым в графической утилите «Управление политикой безопасности».

8 Изменить мандатный уровень доступа с использованием графической утилиты «Управление политикой безопасности».

9 Вынести в терминал *Fly* параметры мандатного управления доступом и мандатного контроля целостности.

Контрольные вопросы

1 Какие уровни доступа и иерархические категории создаются при установке ОССН?

2 Как добавить новые уровни доступа и иерархические категории?

3 Каковы особенности удаления и модификации уровней доступа и иерархических категорий в ОССН?

4 Какие команды используются для создання, модификации и удаления уровней доступа и иерархических категорий в ОССН?

5 Какие команды используются для настройки привилегий учётных записей пользователей?

6 Как принудительно удалить привилегии для заданной учётной записи пользователя?

Лабораторная работа № 3. Мандатное управление доступом в файловой системе

Цель работы: получить навыки администрирования мандатного управления доступом и контроля целостности в файловых системах *Ext2* / *Ext3* / *Ext4* в ОССН и навыки использования для этого графической утилиты «Управление политикой безопасности», менеджера файлов, а также консольных команд.

Общие положения

В ОССН мандатное управление доступом интегрировано в файловую систему за счёт хранения в ней не только дискреционных прав доступа, но и мандатных меток файлов с дополнительными специальными атрибутами. Параметрами мандатного управления доступом (мандатной меткой) каждой сущности файловой системы являются:

– уровень конфиденциальности;

– уровень целостности:

– набор неиерархических категорий;

– специальные атрибуты.

Наличие у сущности файловой системы мандатных меток целостности позволяет дополнительно усилить защиту от несанкционированной модификации файлов, влияющих на безопасность ОССН. Это реализуется установкой уровня целостности «Высокий», что позволяет предотвратить изменение или удаление таких файлов процессами с низким уровнем целостности.

Практическое задание

1 Начать работу в графическом режиме с учётной записью пользователя *user* (уровень доступа – 0, неиерархические категории – нет, уровень целостности – «Низкий»).

2 Создать неиерархические категории с использованием графической утилиты «Управление политикой безопасности». Дня этого выполнить следующие действия: в разделе «Категории» создать следующие новые неиерархические категории: «Группа_1» со значением «Разряд», равным 0, «Группа_2» со значением «Разряд», равным 1, «Группа _3» со значением «Разряд», равным 2.

3 Создать новую группу с именем *office1* с использованием графической утилиты «Управление политикой безопасности».

4 Создать новые учётные записи пользователей *user1*, *user2*, *user3*.

5 Изучить особенности однопользовательской работы с сущностями файловой системы на различных мандатных уровнях доступа и с различными наборами неиерархических категорий с использованием графической утилиты *fly-fm*.

6 Выполнить вывод мандатных меток конфиденциальности и целостности файлов 01.txt, 11.txt, 21.txt с использованием графической утилиты *fly-fm*.

7 Изучить особенности многопользовательской работы с сущностями файловой системы на различных уровнях доступа и целостности и с различными наборами неиерархических категорий.

Контрольные вопросы

1 Какие команды используются для изменения и просмотра параметров мандатного управления доступом файлов?

2 Как организовано хранение файлов в домашних каталогах учётных записей пользователей при работе на различных уровнях доступа?

3 Какие параметры мандатного управления доступом устанавливают по умолчанию при создании файлов и каталогов?

Лабораторная работа № 4. Аутентификация пользователей в системе. Работа с модулями PAM

Цель работы: получить практический опыт настройки системы аутентификации (в том числе двухфакторной) в ОССН с использованием модулей PAM (Pluggable Authentication Modules).

Общие положения

Для подключённых модулей PAM их конфигурирование выполняется путем редактирования файлов в каталогах */etc/security* и */etc/pam.d*. При использовании аутентификации с использованием PAM формируется стек модулей обработки запроса на аутентификацию. Например, в ОССН имеется модуль *pam_limits.so* (с конфигурационным файлом */etc/security/limits.conf*), позволяющий задавать для учётных записей пользователей ограничения на параметры работы функционирующих от их имени процессов, или модуль *pam.cracklib.so*, реализующий правила формирования новых паролей учётных записей пользователей, что позволяет ограничивать минимальную длину пароля, задавать сложность пароля и другие параметры.

В ОССН реализованы следующие типы модулей PAM:

– auth – модули аутентификации;

– account – модули управления учётными записями пользователей;

– session – модули управления сеансами;

– password – модули управления паролями учётных записей пользователей.

При реализации двухфакторной аутентификации электронный идентификатор (ЭИ) должен быть совместим с ОССН. Кроме того, для работы с ЭИ необходима установка дополнительных пакетов, содержащих драйверы или иные необходимые для функционирования ЭИ файлы.

При проверке корректности двухфакторной аутентификации с использованием ЭИ необходимо оставлять возможность штатной аутентификации. В противном случае, например, при неправильной настройке ЭИ, вход в систему с использованием штатной аутентификации будет невозможен и потребуется восстановление ОССН.

Для работы с модулями PAM и ЭИ используются следующие команды:

– *pam-auth-update* – команда управления активными профилями PAM;

– *passwd* – команда смены пароля учётной записи пользователя;

– *pkcs15-tool* – команда для работы с параметрами ЭИ;

– *pkcs15-init* – команда инициализации ЭИ;

– *openssl* – команда для работы с ключевой информацией и ЭИ.

Практическое задание

1 Начать работу в графическом режиме с учётной записью пользователя *user* (уровень доступа – 0, неиерархические категории – нет, уровень целостности – «Низкий») и запустить терминал *Fly* в привилегированном режиме командой *sudo fly-term*.

2 Определить модули PAM, установленные в ОССН, командой *find / -name "pam_*.so"* и выяснить их расположение в каталогах ОССН.

3 Проанализировать текущие настройки PAM в файле *etc/pam.conf* командой *less /etc/pam.con*f.

4 Перейти в каталог */etc/pam.con*f для настройки модулей PAM. Считать список файлов сценариев аутентификации командой *ls –l.*

5 Проанализировать общие настройки аутентификации по файлу */etc/pamd/common-auth*, выполнив команду *less common-auth*.

6 Проверить настройки паролей, для этого выполнить следующие действия:

– запустить графическую утилиту «Управление политикой безопасности» и открыть раздел «Глобальная политика»;

– сравнить значения параметров использования паролей, заданные во вкладке «Параметры изменения пароля» и в файле */etc/login.defs*, во вкладке «Параметры структуры поля» и в файлах *cracklib* и *common-password*.

7 Выполнить смену пароля учетной записи текущего пользователя командой *passwd* и ввести старый пароль, а затем проверить параметры паролей путём его смены и просмотра предупреждающих сообщений.

8 Проверить работу двухфакторной аутентификации на различных уровнях доступа.

Контрольные вопросы

1 Какие типы модулей PAM поддерживаются в ОССН?

2 Каким образом осуществляется обработка стека модулей PAM при аутентификации от имен и учетных записей пользователей в ОССН?

3 Какими командами создаются ключевые пары на ЭИ?

Лабораторная работа № 5. Настройка механизмов организации замкнутой программной среды

Цель работы: изучить принципы и технологии контроля целостности средств защиты (КСЗ), реализованных в ОССН; освоить умения, необходимые для решения задач контроля целостности и создания замкнутой программной среды.

Общие положения

Механизм замкнутой программной среды позволяет ограничить доступ пользователей к исполняемым файлам только теми программами, которые необходимы им для работы.

При использовании этого механизма действуют следующие правила:

– пользователь может запустить программу только из списка разрешенных для запуска программ (*UEL*-список, *User Executable List*). Этот список формируется индивидуально для каждого пользователя;

– замкнутая программная среда может быть включена выборочно для отдельных пользователей;

– замкнутая программная среда может использоваться в одном из двух режимов работы: «мягком» или «жестком».

При «мягком» режиме пользователю разрешается запускать любые программы, а не только входящие в UEL-список. При этом в журнале безопасности регистрируются соответствующие события несанкционированного доступа (НСД).

При «жестком» режиме запуск программы разрешается, если:

– разрешен запуск файла в *UEL*-списке;

– файл не доступен текущему пользователю на изменение;

– файл не находится на сменном носителе;

– владельцем файла является локальная группа администраторов (это дополнительное ограничение, которое может и не использоваться).

Механизм контроля целостности исполняемых файлов и разделяемых библиотек формата ELF при запуске программы на выполнение реализован в модуле ядра ОС *digsig_verif*, который является невыгружаемым модулем ядра ОССН и может функционировать в одном из следующих режимов:

– исполняемым файлам и разделяемым библиотекам с неверной электронной цифровой подписью (ЭЦП), а также без ЭЦП загрузка на исполнение запрещается (штатный режим функционирования);

– исполняемым файлам и разделяемым библиотекам с неверной ЭЦП, а также без ЭЦП загрузка на исполнение разрешается, при этом выдается сообщение об ошибке проверки ЭЦП (режим для проверки ЭЦП);

– ЭЦП при загрузке исполняемых файлов и разделяемых библиотек не проверяется (отладочный режим для тестирования).

Механизм контроля целостности файлов при их открытии на основе ЭЦП в расширенных атрибутах файловой системы также реализован в модуле ядра ОС *digsig_verif* и может функционировать в одном из следующих режимов:

– запрещается открытие файлов, поставленных на контроль, с неверной ЭЦП или без ЭЦП;

– открытие файлов, поставленных на контроль, с неверной ЭЦП или без ЭЦП разрешается, при этом выдается сообщение об ошибке проверки ЭЦП (режим для проверки ЭЦП в расширенных атрибутах файловой системы);

– ЭЦП при открытии файлов не проверяется.

Практическое задание

1 Запустить терминал *Fly* в «привилегированном» режиме командой *sudo fly-term*.

2 Просмотреть загруженные модули ядра ОССН и вынести в терминал данные о невыгружаемом модуле *digsig_verif* конвейером команд *lsmod | grep digsig-verif*.

3 Выполнить импорт открытых ключей, используемых для проверки ЭП файлов. Для этого выполнить следующие действия:

– инициализировать каталог */roof/.gnupg* при просмотре текущих ключей командой *gpg --list-sigs*;

– импортировать открытый мастер-ключ «NPO RusBITech» командой *gpg --import /etc/digsig/primary_key.gpg*;

– импортировать открытый ключ «ССТ RusBITech», используемый для ЭП файлов, командой *gpg --import /etc/digsig/key_for_signing.gpg*.

4 Вывести текущие ключи командой *gpg --list-sigs*. Определить идентификатор мастер-ключа.

Контрольные вопросы

1 Каким вариантом модулей ядра ОССН является модуль *digsig.verif*?

2 Какой формат файлов ключей ЭП СПО использует модуль *digsig.verif*?

3 Какой файл сценария командного интерпретатора *bash* применяется для хранения ключей ЭП для модуля *digsig.verif*?

4 Связан ли модуль *digsig.verif* с другими загружаемыми (невыгружаемыми) модулями?

Лабораторная работа № 6. Настройка сетевого взаимодействия

Цель работы: изучить принципы и порядок конфигурирования сетевого взаимодействия узлов автоматизированной системы в защищенном исполнении (АСЗИ) на базе ОССН; освоить навыки решения задач управления сетевыми интерфейсами и протоколами, а также маршрутизацией пакетов.

Общие положения

Взаимодействие узлов АСЗИ между собой и с сетевым оборудованием в сетях с пакетной коммутацией на базе стека протоколов TCP/IP основано на сетевых службах, реализуемых соответствующими процессами в ОССН. Такие процессы на серверных узлах АСЗИ создают программные интерфейсы (сокеты), связанные с требуемыми сетевыми службами сетевыми портами. Процессы ОССН на клиентских узлах АСЗИ формируют запрос на открытие соответствующего сокета с указанием IP-адреса и сетевого порта серверных узлов АСЗИ. Результатом выполнения такого запроса является установление соединения между серверными и клиентскими узлами ОССН в рамках заданной сетевой службы.

Особенностью этого соединения в ОССН является поддержка передачи по нему данных мандатного контекста сущностей сетевой службы и субъектов доступа к ней. При этом монитором обращений выступает подсистема безопасности *PARSEC*. В случаях, когда сетевой сервис не обрабатывает данные мандатного контекста, однако осуществляет соединение с процессами ОССН, работающими в различных мандатных контекстах, применяется механизм *privsock*.

Конфигурация сетевых интерфейсов, настройка адресной информации и статической маршрутизации пакетов реализуются наборами команд *Net tools* (пакет *nettools*) и *Iproute2* (пакет *iproute*), графической утилитой *fly-admin-device-manager* и командой *cthtool*. Для статического конфигурирования параметров сетевых интерфейсов также используется конфигурационный файл */etc/network/interfaces*, а для управления запуском программ перед инициализацией и закрытием сетевых интерфейсов – наборы сценариев, расположенные в каталогах */etc/network/if-np.d*, */etc/network/if-down.d*, */etc/if-pre-up.d* и */etc./if-post-down.d.*

Практическое задание

1 Начать работу со входа в ОССН *AstraClient1*, *AstraClient2* и *AstraRouter* в графическом режиме с учётной записью пользователя *user* (уровень доступа – 0, неиерархические категории – нет, уровень целостности – «Низкий»).

2 В ОССН *AstraClient1*, *AstraClient2* и *AstraRouter* запустить терминал *Fly* в привилегированном режиме командой *sudo fly-term* и вывести информацию о доступных сетевых интерфейсах командой *ip link list*.

3 Настроить ОССН *AstraClient1*.

4 Выполнить настройки сетевого интерфейса ОССН *AstraClient2*.

5 В ОССН *AstraRouter* выполнить настройку статических сетевых адресов и маршрутизации.

6 Проверить функционирование маршрутизации между подсетями.

7 Выполнить настройки сетевых интерфейсов в ОССН *AstraClient1* с использованием графической утилиты «Сетевые соединения».

8 Проверить совместную работу программ конфигурирования сетевых интерфейсов в ОССН *AstraClient1*.

9 Настроить DNS-сервер в ОССН *AstraRouter* для работы с использованием механизма */network*.

10 Проверить работу ОССН *AstraClient1* с DNS-сервером в сессии, функционирующей от имени учётной записи пользователя *user* с мандатным уровнем доступа, равным 2.

Контрольные вопросы

1 Укажите назначение пакета *inroute*.

2 Какие основные команды входят в пакет *inroute*?

3 Каковы отличительные особенности пакетов *inroute* и *net-toole*?

Лабораторная работа № 7. Конфигурирование службы AstraLinuxDirectory

Цель работы: получить практический опыт установки и настройки параметров службы Astra Linux Directory (ALD) в ОССН.

Общие положения

В компьютерных сетях, построенных на основе ОССН, имеется возможность организовать централизованное хранение учётных записей пользователей в домене *ALD* (далее – домене), а также развёртывать централизованный защищенный файловый сервер, содержащий сетевые домашние каталоги данных учётных записей пользователей. Таким образом, у учётных записей пользователей *ALD* появляется возможность регистрации и доступа к своим сетевым объектам с любого компьютера, входящего в домен. Это особенно актуально в случае территориальной удалённости между контроллером *ALD* и компьютерами, входящими в состав домена.

Администратор домена выполняет следующие функции по управлению доменом:

– централизованное управление учётными записями пользователей домена с использованием команды *ald-admin* и графической утилиты «Управления политикой безопасности»;

– настройка СЗИ, управляющих их доступом к файловым сущностям защищенного файлового сервера.

Служба *ALD* обладает расширяемой архитектурой, состоящей из ядра, отвечающего за основной функционал системы, ряда интерфейсов (*LDAP*, *Kerberos*) и модулей расширения, команд и графических утилит настройки служб и подсистем *ALD*, что позволяет расширять функциональность *ALD*, устанавливая дополнительные пакеты.

На компьютере, осуществляющем функции контроллера *ALD*, операции по администрированию *ALD* выполняются от имени учётных записей пользовате-

лей, обладающих соответствующими административными полномочиями. В зависимости от назначенных привилегий администраторов *ALD* можно разделить на следующие группы по полномочиям:

– корневой администратор (имя *admin/admin*, администратор *ALD*) обладает всеми полномочиями по управлению доменом;

– администраторы (пользователи с привилегией *admin*) обладают полномочиями по управлению конфигурацией домена и учётными записями пользователей;

– ограниченные администраторы (учётные записи пользователей с привилегиями *hosts-add* или *all-hosts-add*) обладают полномочиями по добавлению компьютеров в домен;

– пользователи утилит администрирования (пользователи с привилегией *adm-user*) обладают полномочиями по запуску утилит администрирования;

– обычные пользователи.

Для администрирования домена используются команды *ald-admin* и графическая утилита «Управление политикой безопасности».

Практическое задание

1 Для настройки сетевого соединения на контроллере и клиентах *ALD* начать работу со входа в ОССН *AstraClient1*, *AstraClient2* и *AstraServer* в графическом режиме с учётной записью пользователя *user* (уровень доступа – 0, неиерархические категории – нет, уровень целостности – «Низкий»).

2 В ОССН *AstraClient1, AstraClient2* и *AstraServer* выполнить настройку статических сетевых адресов.

3 Выполнить проверку корректности настроек командой *ping*. При этом проверить доступность *AstraClient1*, *AstraClient2* с *AstraServer* по сети командами *ping 10.0.0.1* и *ping 10.0.0.2*. Затем проверить доступность *AstraClientl* с *AstraClient2* командой *ping 10.0.0.1*. В каждом случае количество полученных «*recieved*»-пакетов должно соответствовать количеству отосланных «*transmitted*».

4 Выполнить установку, конфигурирование, запуск клиентов *ALD*.

5 Осуществить проверку функционирования и настройку контроллера и клиентов *ALD*.

6 Создать новую учётную запись пользователя *ALD* и осуществить вход с неё в ОССН *AstraClient1*.

Контрольные вопросы

1 Каково назначение служб контроллера *ALD*?

2 Какие службы устанавливаются на контроллер *ALD*?

3 Каковы особенности настройки имен компьютеров, входящих в домен?

Лабораторная работа № 8. Управление программными пакетами. Настройка системных служб

Цель работы: освоить администрирование пакетов ОССН, в том числе используемых для этого команд и графических утилит, а также администрирование и настройку системных служб.

Общие положения

Система управления пакетами ОССН включает несколько команд и утилит, которые могут работать в режиме командной строки, в псевдографическом и графическом режимах. При этом порядок действий при их использовании для изменения состава установленных в ОССН пакетов принципиально не отличается, за исключением, возможно, установки взаимосвязанных пакетов.

Для управления пакетами применяются утилиты *aptitude*, «Менеджер пакетов *Synaptic*», команды системы управления пакетами *APT* и команда *dpkg*.

Для управления запуском системных служб используется команда *service имя_службы <команда>*. В качестве параметров команды применяются *start*, *stop*, *restart*, *status* для запуска, останова, перезапуска или определения статуса системной службы соответственно. Просмотр уровней запуска системных служб может быть осуществлён с использованием команд *service --status-all* или более наглядной *chkcontig -list*. Для включения/отключения системной службы на конкретном уровне может быть использована команда *chkconfig имя-службы <on|off>*. Аналогичные функции реализует графическая утилита *fly-admin-runlevel*.

Практическое задание

1 Начать работу в ОССН в графическом режиме учётной записью пользователя *user* (уровень доступа – 0, неиерархические категории – нет, уровень целостности – «Низкий»).

2 Запустить терминал *Fly* и перейти в каталог */etc/apt*.

3 Вывести дискреционные права доступа к файлу *sources.list* командой *ls-l sources.list*. Определить возможность изменения файла при работе от имени данной учётной записи пользователя.

4 Запустить второй терминал *Fly* командой *sudo fly-term* и в нём выполнить команду *aptitude*.

5 В первом терминале выполнить попытку удаления пакета *ed* командой *apt-get remove ed*, проанализировать выводимые ошибки.

6 Завершить *aptitude* во втором терминале. В первом терминале повторить удаление пакета *ed* командой *apt-get remove ed*. Проанализировать отображаемые в терминале сообщения и определить количество удаленных пакетов.

7 Выполнить проверку статуса установленных пакетов, для чего осуществить следующие действия:

– в привилегированном режиме терминала *Fly* запустить утилиту *aptitude* и проанализировать предупреждения;

– нажать клавишу «c» для просмотра первого решения об установке пакета *vim-common*;

– выполнить просмотр следующего решения и выйти из утилиты *aptitude*.

8 Выполнить настройку пакетов в графической утилите *Synaptic*, для чего осуществить следующие действия:

– запустить графическую утилиту *Synaptic*, при этом ввести пароль текущей учётной записи пользователя для возможности работы в привилегированном режиме;

– открыть меню «Настройки/Репозитории» и проверить наличие неактивного репозптория, который был ранее закомментирован в файле *sources.li*st;

– удалить неактивный и активный репозитории.

9 Для управления системными службами выполнить следующие действия:

– в привилегированном режиме терминала *Fly* получить текущие статусы запускаемых системных служб командой *service_status-all*;

– определить статус системной службы *nfs-kernel-server* командой *service nfs-kernel-server status*;

– выполнить попытку определения статуса системной службы *console-setup* командой *service console-setup status* и проанализировать результат;

– для анализа порядка вызова команды *service* вывести на экран содержимое файла *console-setup* командой *cat /etc/init.d console-setup*;

– аналогично по содержимому файла *console-setup* найти реализацию вызова команды *status*.

Контрольные вопросы

1 Каковы особенности одновременной работы нескольких утилит управления пакетами?

2 Какие команды позволяют работать с зависимыми пакетами в автоматическом режиме?

3 Как определить статус запуска системной службы?

Лабораторная работа № 9. Контроль целостности комплекса средств зашиты

Цель работы: изучить принципы и технологии контроля целостности комплекса средств защиты (КСЗ), реализованных в ОССН.

Общие положения

АСЗИ на базе ОССН должны обеспечивать функции как аудита доступа к сущностям файловой системы, так и контроля целостности (*integrity*) данных и содержимого исполняемых файлов.

Подобный контроль позволяет с достаточной уверенностью констатировать факт отсутствия в данных, обрабатываемых системными процессами ОССН, недекларируемых для АСЗИ возможностей.

Для решения задачи контроля целостности в состав КСЗ ОССН включены средства, реализующие частные функции управления целостностью данных:

– вычисления и проверки контрольных сумм файлов и оптических дисков:

– контроля соответствия дистрибутиву;

– регламентного контроля целостности.

Контрольная сумма – значение, рассчитанное по набору данных путём применения определённого алгоритма и используемое для проверки целостности данных при их передаче или хранении. Она используется для быстрого сравнения двух наборов данных на эквивалентность: с большой вероятностью отличающиеся наборы данных будут иметь разные контрольные суммы.

Проверка соответствия модулей установленной ОССН модулям, входящим в состав её дистрибутива, является вариантом статического контроля целостности и обеспечивает контроль целостности файловых сущностей, копируемых в корневой раздел ОССН на этапе установки, что позволяет убедиться в отсутствии изменений в файловых сущностях модулей, произошедших на этапе их эксплуатации.

Практическое задание

1 Начать работу со входа в ОССН в графическом режиме с учетной записью пользователя *user* (уровень доступа – 0, неиерархические категории – нет, уровень целостности – «Низкий») и запустить терминал *Fly* в привилегированном режиме командой *sudo fly-term*.

2 В домашнем каталоге создать подкаталог *checksum* и скопировать в него все файлы (исключая вложенные каталоги) из каталога */etc*.

3 Используя алгоритм *MD5* вычислить контрольные суммы всех файлов в каталоге */home/user/checksum* и перенаправить результат их вычисления в файл */home/user/md5check*, а поток «перечень ошибок» – в файл */home/user/error.md5*.

4 Используя алгоритм *SHA-512/256*, вычислить контрольные суммы всех файлов в каталоге */home/user/checksum*.

5 Изменить содержимое файла /*etc/fstab*, удалив в нем две первые строки.

6 Запустить графическую утилиту «Контроль целостности файлов» (*afick-tk*) управления системой *AFICK* из меню «Системные» главного пользовательского меню и выполнить принудительную проверку целостности, выбрав действие – сравнение с базой.

7 После завершения контроля целостности в меню утилиты *afick-tk* «Файл-история» определить дату и время последнего принудительного контроля целостности.

8 Проанализировать найденную запись о нарушении целостности п определить параметры, соответствующие действиям (*action*) нарушения целостности, и их текущие значения.

Контрольные вопросы

1 В каких средствах контроля целостности используется библиотека *libgost*?

2 Как инициализировать базу данных системы регламентного контроля *AFICK* после внесения изменений в её конфигурационный файл?

3 Каким образом реализована взаимосвязь системы регламентного контроля целостности *AFICK* и сервиса *cron*?

Список литературы

1 Безопасность операционной системы специального назначения Astra Linux Special Edition: учебное пособие для вузов / П. И. Буренин [и др.]; под ред. П. И. Девянина. – Москва: Горячая линия-Телеком, 2016. – 312 с.

2 **Баранова, Е. К.** Информационная безопасность и защита информации: учебное пособие / Е. К. Баранова, А. В. Бабаш. – 4-е изд., перераб. и доп. – Москва: РИОР, ИНФРА-М, 2018. – 336 с.