

Установка ПАК СЗИ НСД Аккорд-Х

Требования к системе

Дистрибутив ОС	Red Hat Enterprise Linux 5.4
Архитектура	i386
Версии ядра Linux	<ul style="list-style-type: none">• 2.6.18-164.el5, пересобранное с опциями, указанными в руководстве по установке;• 2.6.18-164.el5.accordx, идущее в комплекте с Аккорд-Х
Загрузочное устройство	hd*, sd*
Конфигурация разделов	/boot: ext2,ext3; /: ext2, ext3; остальные разделы: любые ФС, поддерживаемые ядром Linux
Версия gtk+	>= 2.12
Версия pygtk	>= 2.12

Руководство по установке

1 Проверка выполнения требований к системе

До начала установки необходимо убедиться, что система удовлетворяет требованиям, приведенным в «требованиях к системе».

2 Установка монитора разграничения доступа асрип

2.1 Для работы монитора разграничения доступа необходимо использовать модифицированное ядро Linux. Есть два варианта:

а) Использовать уже готовое ядро, идущее в поставке данным ПО. Пакет с готовым ядром называется *kernel-2.6.18-164.el5.accordx.i686.rpm*. Для установки пакета необходимо выполнить команду

```
rpm -ivh kernel-2.6.18-164.el5.accordx.i686.rpm
```

б) Пересобрать ядро, распространяемое с дистрибутивом ОС, изменив следующие параметры файла конфигурации ядра:

1. Значение CONFIG_SECURITY_CAPABILITIES изменить с 'y' на 'm';
2. Значение CONFIG_SECURITY_SELINUX_BOOTPARAM_VALUE изменить с '1' на '0'.

После внесения изменений в файл конфигурации ядра необходимо пересобрать и установить ядро в соответствии с руководством администратора дистрибутива ОС.

2.2 После того, как ядро установлено, необходимо заменить автоматически сгенерированный образ начальной загрузки файлом *initrd-2.6.18-164.el5.accordx.img*.

3 Установка утилит администрирования

В состав тестовой версии комплекса входят утилиты просмотра журналов и БД пользователей.

Для установки утилит администрирования необходимо выполнить команду

```
rpm -ivh accordx-admin-b0-0.i686.rpm
```

При успешном завершении процесса установки в каталоге */opt/accordx/* появятся исполняемые файлы утилит *dbview* и *logview*. Для запуска утилит необходимо перейти в каталог */opt/accordx/* и запустить нужный исполняемый файл:

```
cd /opt/accordx  
./dbview  
./logview
```

4 Настройка записей пользователей

В тестовой версии комплекса редактирование настройка записей пользователей осуществляется путем редактирования файла БД пользователей с помощью любого текстового редактора.

БД пользователей должна находиться в файле */etc/opt/accordx/userdb.acx*.

Описание формата БД пользователей

Файл базы данных записан в текстовом формате. Синтаксис базы данных приведен ниже (Служебные символы \t — табуляция, \n — перевод строки.)

```
корневой ключ: \t значение\n  
    \t ключ: \t значение\n  
    \t ключ# \t переменная \t значение\n  
    \t ключ:\n  
    \t \t значение1\n  
    \t \t значение2\n  
    . . .  
\n  
    \t ключ# \n  
    \t \t переменная1 \t значение1\n  
    \t \t переменная2 \t значение2\n  
    . . .  
\n
```

«корневой ключ» может принимать значения *user*, *group*, *process*. Корневые записи разделены пустой строкой.

В каждой корневой записи может содержаться одна или несколько записей одного из четырех типов:

- одиночное значение;
- переменная — значение;
- список одиночных значений;
- список переменная — значения.

Одиночные значения и списки одиночных значений идентифицируются символом двоеточие «:» после ключа. Записи типа переменная — значение идентифицируются символом «#». Если после ключа сразу следует перевод строки, то это воспринимается как идентификатор списка. Каждый элемент списка стоит на отдельной строке и отделяется дополнительным символом табуляции. Список должен заканчиваться пустой строкой.

Пример БД находится в `/etc/opt/accordx/userdb.acx.sample`

Ниже приведена таблица с описанием ключей БД и их значений.

Ключ	Значение
user:	Корневой ключ, обозначающий начало записи пользователя
comment:	Комментарий к записи
pass_change_day:	Дата следующей смены пароля
is_blocked:	Запись заблокирована
group:	Группа, в которую входит запись
UID:	Идентификатор пользователя в ОС (uid)
is_superuser:	Является ли запись записью администратора
working_time#	Допустимые часы работы
pass_symbols#	Символы, которые должны обязательно присутствовать в пароле
acl#	Правила разграничения доступа
key:	Открытый ключ пользователя
pass_gen:	Флаг необходимости генерации пароля
ia_results#	Результаты прохождения процедуры идентификации/аутентификации в контроллере, передаваемые в ОС
change_try:	Максимально возможное количество попыток смены пароля
icl:	Список контроля целостности
pass_ttl:	Время жизни пароля
tm_ind:	ТМ-идентификатор
pass_len:	Минимальная длина пароля