ВОЕННО-КОСМИЧЕСКАЯ АКАДЕМИЯ ИМЕНИ А.Ф.МОЖАЙСКОГО
Кафедра № 27 Математического и программного обеспечения

УТВЕРЖДАЮ
Начальник 27 кафедры
полковник
С. Войцеховский
«___» _____ 2022 г.

Практическое занятие № 13
по учебной дисциплине
«Защита информации»
на тему:

Особенности работы с ПО РМ АОБИ «Система защиты от НСД» ОС МСВС 3.0

Рассмотрено и одобрено
на заседании кафедры № 27
« ___ » _____ 202_ г. протокол № ___

Санкт-Петербург
2022

Содержание занятия и время

Введение – 10 мин.

1. Установка сервера и агента домена безопасности ОС МСВС 3.0. - 30 мин
2. Включение АРМ клиентов ПО РМ АОБИ и пользователей в домен безопасности МСВС 3.0. 30 мин.

Заключение и указания по отработке материала лекции – 5 мин.

Литература

Основная:

1. Войцеховский С.В., Калиниченко С.В. Архитектура и программное обеспечение современных компьютерных систем и сетей ВКС. – СПб.: ВКА имени А.Ф. Можайского, 2013. – 352 с.

2. Войцеховский С.В. Практикум по дисциплине «Архитектура и программное обеспечение современных компьютерных систем и сетей» . – СПб.: ВКА имени А.Ф. Можайского, 2015. – 119 с.

Дополнительная:

3. Колисниченко Д. Н. FreeBSD. От новичка к профессионалу. – СПб.: БХВ-Петербург, 2011. – 544 с.

Материально-техническое обеспечение

1. Программное обеспечение: Oracle Virtual Box 4.2.12. Дистрибутив программ КСЗИ СВАС;
2. Технические средства обучения – ПЭВМ.

Вопрос № 1

«УСТАНОВКА СЕРВЕРА ДОМЕНА БЕЗОПАСНОСТИ ОС МСВС 3.0.»

Порядок работы:

1. Предназначение и установка сервера домена безопасности ОС МСВС 3.0.

Сервер домена безопасности ОС МСВС 3.0 входит в состав ПО РМ АОБИ и является его основным компонентом.

Предназначение ПО РМ АОБИ:

- для обеспечения централизованного контроля доступа в АС;
- идентификации и проверки подлинности субъектов доступа при входе в систему по идентификатору (коду) и паролю временного действия длиной не менее восьми символов;
- идентификации ПЭВМ, узлов сети, программ, томов, каталогов, файлов по именам;
- формирования учетных записей пользователей;
- установки и модификации меток конфиденциальности субъектов доступа;
- тиражирования производимых настроек политики безопасности на определенные администратором безопасности АРМ из состава АС;
- блокировки на вход ПЭВМ всех пользователей при совершении несанкционированного доступа на данной ПЭВМ;
- регистрации входа (выхода) субъектов доступа в систему (из системы);
- регистрации запуска (завершения) всех программ и процессов (заданий, задач) в АС, которые не входят в список разрешенных к запуску;
- регистрации попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам, список которых определяется администратором безопасности;

- регистрации попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым устройствам (ЭВМ, терминалы, линии связи и т.д.), список которых определяется администратором безопасности;
- регистрации действий администратора безопасности по изменению полномочий субъектов доступа и статуса объектов доступа;
- контроля целостности файлов, список которых определяется администратором безопасности, при запуске системы по именам и контрольным суммам;
- периодического контроля целостности файлов по именам и контрольным суммам в процессе работы ОС, периоды проверки определяются администратором.

К серверу ПО РМ АОБИ прилагается визуальная система администрирования настроек безопасности АС, предназначенная для удобного управления сервером.

2. Установка и запуск сервера домена безопасности ОС МСВС 3.0.

Установка сервера ПО РМ АОБИ и визуальной системы администрирования:

[root@mcbc3server /]# **rpm -ihv /mnt/cdrom/461829.001/00006-01/mycom-bin-1.0-2.i386.rpm**
[root@mcbc3server /]# **rpm -ihv /mnt/cdrom/461829.001/00006-01/AOBI-rm-1.0-16cbit.i386.rpm**

Для настройки автозапуска сервера ПО РМ АОБИ при загрузке системы, следует ввести команду:

[root@mcbc3server /root]# **chkconfig --level 345 aobiserver on**
[root@mcbc3server /]# **chkconfig --list aobiserver**
aobiserver 0:выкл 1:выкл 2:выкл 3:вкл 4:вкл 5:вкл 6:выкл

Для запуска и останова сервера ПО РМ АОБИ вручную применяются следующие команды:
- для запуска ввести команду **«service aobiserver start»** или **«/etc/init.d/aobiserver start»;**
- для останова ввести команду **«service aobiserver stop»** или **«/etc/init.d/aobiserver stop»**.

Запуск визуальной системы администрирования осуществляется из графического оконного интерфейса:

- вызвать диалоговое окно ввода команд **(Alt+F2)**
- ввести команду **«usd»** и нажать клавишу **«Enter».**

В случае успешного запуска на экране должно появиться главное рабочее окно программы (рис. 11). При этом, запуск визуальной среды администрирования ПО РМ АОБИ должен осуществляться после запуска сервера ПО РМ АОБИ. Если сервер ПО РМ АОБИ не запущен, то после запуска визуальной среды администрирования ПО РМ АОБИ будет выведено окно с соответствующим сообщением.

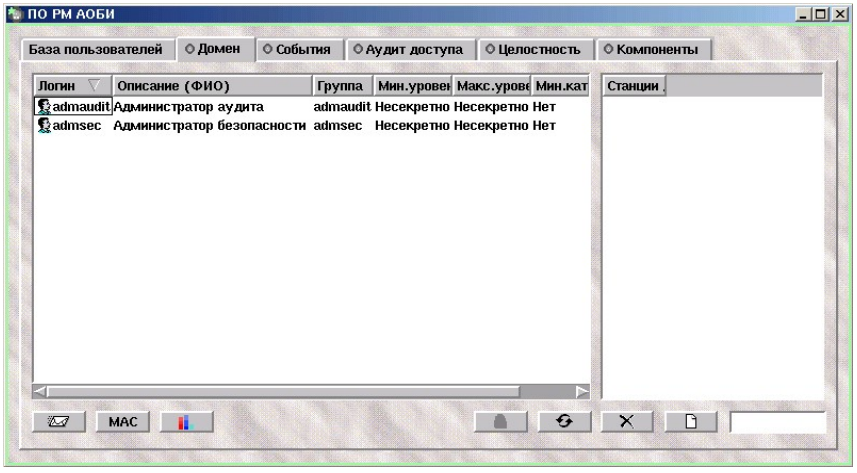


Рис. 11. Главное рабочее окно программы

Вопрос № 2

«УСТАНОВКА АГЕНТА ДОМЕНА БЕЗОПАСНОСТИ ОС МСВС 3.0.»

Порядок работы:

1. Предназначение и установка агента домена безопасности ОС МСВС 3.0.

Агент домена безопасности ОС МСВС 3.0 входит в состав ПО РМ АОБИ и устанавливается на все клиентские АРМ для обеспечения взаимодействия с сервером ПО РМ АОБИ.

1. Установка агента ПО РМ АОБИ

Установка агента ПО РМ АОБИ:

[root@mcbc3client /]# **mount /mnt/cdrom**
[root@mcbc3client /]# **rpm -ihv /mnt/cdrom/461829.001/00006-01/mycom-bin-1.0-2.i386.rpm**
[root@mcbc3client /]# **rpm -ihv /mnt/cdrom/461829.001/00006-01/AOBI-agent-2.0-12cbit.i386.rpm**

Для настройки автозапуска агента ПО РМ АОБИ при загрузке системы, следует ввести команду:

[root@mcbc3client /]# **chkconfig --level 345 aobiagent on**
[root@mcbc3client /]# **chkconfig --list aobiagent**
aobiagent 0:выкл 1:выкл 2:выкл 3:вкл 4:вкл 5:вкл 6:выкл

Для запуска и останова агента ПО РМ АОБИ вручную применяются следующие команды:

- для запуска ввести команду **«service aobiagent start»** или **«/etc/init.d/aobiagent start»;**
- для останова ввести команду **«service aobiagent stop»** или **«/etc/init.d/aobiagent stop».**

3. Подготовка к работе агента ПО РМ АОБИ

На АРМ клиента ПО РМ АОБИ необходимо указать IP-адрес АРМ сервера ПО РМ АОБИ (возможно, также и дублирующего сервера ПО РМ АОБИ) следующим образом:

[root@mcbc3client /]# **echo >> /usr/local/aobi-agent-m/dau-m.conf “192.168.0.254”**

После этого необходимо перезапустить программу агента ПО РМ АОБИ.

Вопрос № 3

«УСТАНОВКА И УПРАВЛЕНИЕ ДРАЙВЕРОМ ОГРАНИЧЕНИЯ ПОЛНОМОЧИЙ СУПЕРПОЛЬЗОВАТЕЛЯ»

Порядок работы.

1. Предназначение драйвера ограничения полномочий суперпользователя

Драйвер ограничения полномочий суперпользователя предназначен для обеспечения защиты файлов, определенных списком в файле **/etc/downroot.conf** от модификации со стороны суперпользователя. Драйвер ограничения полномочий суперпользователя должен быть установлен на все ЭВМ домена безопасности МСВС 3.0, включая ЭВМ сервера ПО РМ АОБИ.

Перечень файлов в **/etc/downroot.conf** по умолчанию и комментарии к ним:

/var/log/aobimessages — журнал аудита действий суперпользователя ЭВМ сервера ПО РМ АОБИ;

Данный файл имеется в наличии только на ЭВМ сервера ПО РМ АОБИ. Следовательно, суперпользователь ЭВМ сервера ПО РМ АОБИ не сможет удалить или изменить этот файл. В файле **/var/log/aobimessages** хранится информация о действиях суперпользователя при управлении ЭВМ клиентов ПО РМ АОБИ, таких как добавление ЭВМ АС в домен и удаление ЭВМ клиента ПО РМ АОБИ из домена; добавление, тиражирование и удаление пользователей; установка файлов на контроль по целостности и снятие их с контроля.

/etc/downroot.conf — перечень защищенных файлов;

Суперпользователь ЭВМ клиента (сервера) ПО РМ АОБИ не сможет исключить файлы из списка, с целью снять с них защиту.

/etc/passwd — имена и параметры пользователей;

Суперпользователь ЭВМ клиента (сервера) ПО РМ АОБИ не сможет добавить в систему нового пользователя средствами, не входящими в состав ПО РМ АОБИ. Пользователи добавляются методом тиражирования с ЭВМ сервера ПО РМ АОБИ.

/etc/shadow — пароли пользователей в зашифрованном виде;

Суперпользователь ЭВМ клиента (сервера) ПО РМ АОБИ не сможет назначить пользователю пароль средствами, не входящими в состав ПО РМ АОБИ. Пароли назначаются методом тиражирования с ЭВМ сервера ПО РМ АОБИ.

/etc/rc.d/rc.sysinit — самый приоритетный системный сценарий (загрузка модулей ядра и т.д.), выполняющийся при загрузке системы;

В этом сценарии прописывается строка **«/usr/bin/ldownroot»,** которая обеспечивает автозагрузку драйвера ограничения полномочий суперпользователя. Теперь суперпользователь ЭВМ клиента (сервера) ПО РМ АОБИ не сможет отменить загрузку этого драйвера, а также не сможет изменить любой другой параметр в файле **/etc/rc.d/rc.sysinit.**

Примечание: драйвер ограничения полномочий суперпользователя не может быть выгружен в процессе функционирования системы.

/lib/modules/2.2.20-MCBC/misc/downroot.o — файл драйвера ограничения полномочий суперпользователя.

Суперпользователь ЭВМ клиента (сервера) ПО РМ АОБИ не сможет вручную удалить драйвер ограничения полномочий суперпользователя с жесткого диска.

2. Установка драйвера ограничения полномочий суперпользователя

Установка драйвера ограничения полномочий суперпользователя на ЭВМ клиента (сервера) ПО РМ АОБИ:

[root@mcbc3client /root]# **rpm -ihv /mnt/cdrom/461829.001/00006-01/AOBI-downroot-1.0-6cbit.i386.rpm**

Выполнить перезагрузку системы.

3. Управление драйвером ограничения полномочий суперпользователя

В визуальной системе администрирования необходимо перейти к закладке «Компоненты». В левой части отображен список ЭВМ АС. В правой части отображены закладки, каждая из которых отвечает за работу одного компонента.

Открыть закладку «Огран.ROOT» (рис. 12). Компонент «Огран.ROOT» предназначен для удаленного управления драйвером ограничения полномочий суперпользователя.

В верхней части диалога отображена информационная надпись, информирующая администратора о статусе драйвера снижения полномочий суперпользователя на выбранном ЭВМ клиента ПО РМ АОБИ в левой части диалога закладки «Компоненты».

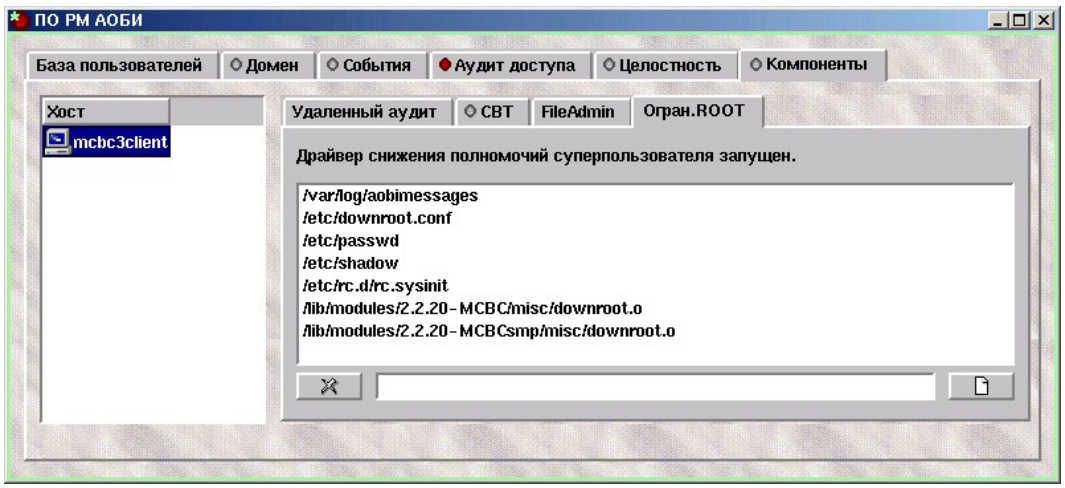


Рис. 12. Диалоговое окно закладки «Огран.ROOT»

В списке диалога компонента «Огран.ROOT» приведен список защищаемых файлов. Добавление и удаление файлов в список защищаемых может осуществляться только через интерфейс ПО РМ АОБИ.

Для добавления файла в список контролируемых необходимо ввести имя файла в строке ввода в нижней части диалога компонента «Огран.ROOT» и нажать кнопку добавления в нижней правой части диалога.

Для снятия защиты с файла необходимо выбрать файл в списке компонента «Огран.ROOT» и нажать кнопку удаления в нижнем левом углу диалога. Появится диалоговое окно подтверждения удаления. При подтверждении защита с выбранного файла будет снята.

Вопрос № 4

«УСТАНОВКА ПРОГРАММЫ ГЕНЕРАЦИИ ПАРОЛЕЙ»

Порядок работы:

1. Предназначение и установка программы генерации паролей

Программа генерации паролей предназначена для генерации и формирования паролей доступа пользователей к сети, файлам, базам данных и другим защищаемым ресурсам на рабочем месте, серверах и других объектах вычислительной техники автоматизированной системы.

Программа генерации паролей осуществляет:

- создание буквенно-цифровых, цифровых паролей длиной от 8 до 16 знаков;
- проверку полученных паролей на удовлетворение криптографическим и инженерно-криптографическим требованиям, предъявляемым к паролям;
- создание на магнитном носителе файла, содержащего сгенерированные пароли;
- распечатку карточек с паролями для выдачи пользователям;
- распечатку журнала учета выдачи карточек.

Установка программы генерации паролей

Программа генерации паролей устанавливается на ЭВМ сервера ПО РМ АОБИ:

[root@mcbc3server /root]# **mount /mnt/cdrom**
[root@mcbc3server /root]# **rpm -ihv /mnt/cdrom/461829.001/00002-01/PGP-1.0-3cbit.i386.rpm**

Запуск программы генерации паролей осуществляется из графической оболочки:

- вызвать диалоговое окно ввода команд (Alt+F2);
- ввести команду «pgp» и нажать клавишу «Enter».

В случае успешного запуска на экране должно появиться рабочее окно программы (рис. 10):

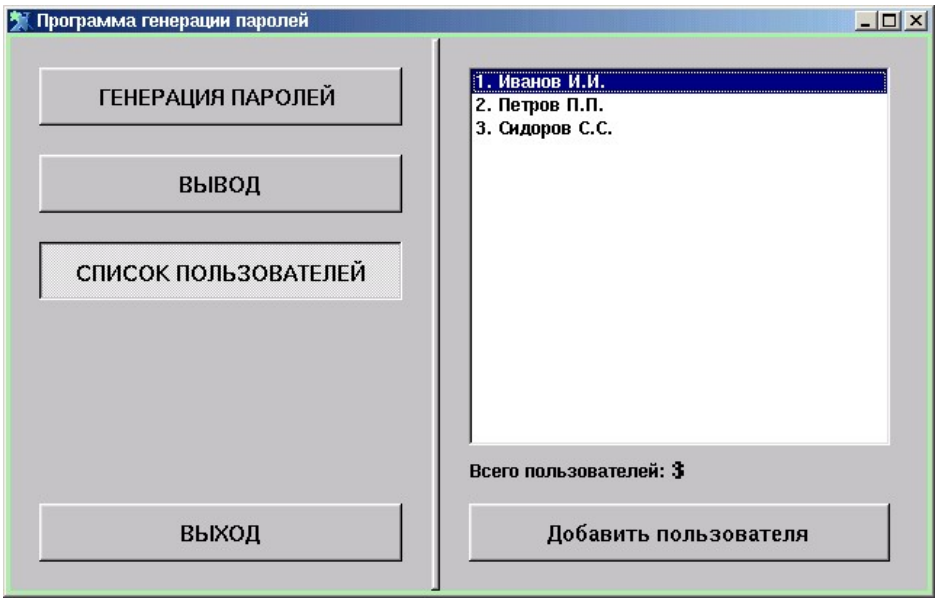


Рис. 10. Диалоговое окно «Программа генерации паролей»

Программа генерации паролей может использоваться отдельно, но в основном применяется в составе визуальной системы администрирования ПО РМ АОБИ.

«УПРАВЛЕНИЕ ПРАВАМИ ПОЛЬЗОВАТЕЛЕЙ С ПОМОЩЬЮ ПО РМ АОБИ»

Порядок работы:

1. Управление дискреционными правами пользователей с помощью ПО РМ АОБИ

Параметры пользователя, принадлежащего базе пользователей АС, могут быть изменены средствами ПО РМ АОБИ, для чего необходимо нажать на кнопку с рисунком **«Пользователи»** в нижней части закладки **«База пользователей».** Появится диалоговое окно редактирования параметров пользователя. Окно содержит три закладки: **«Основные», «Пароль»** и **«Безопасность» (**рис. 18).

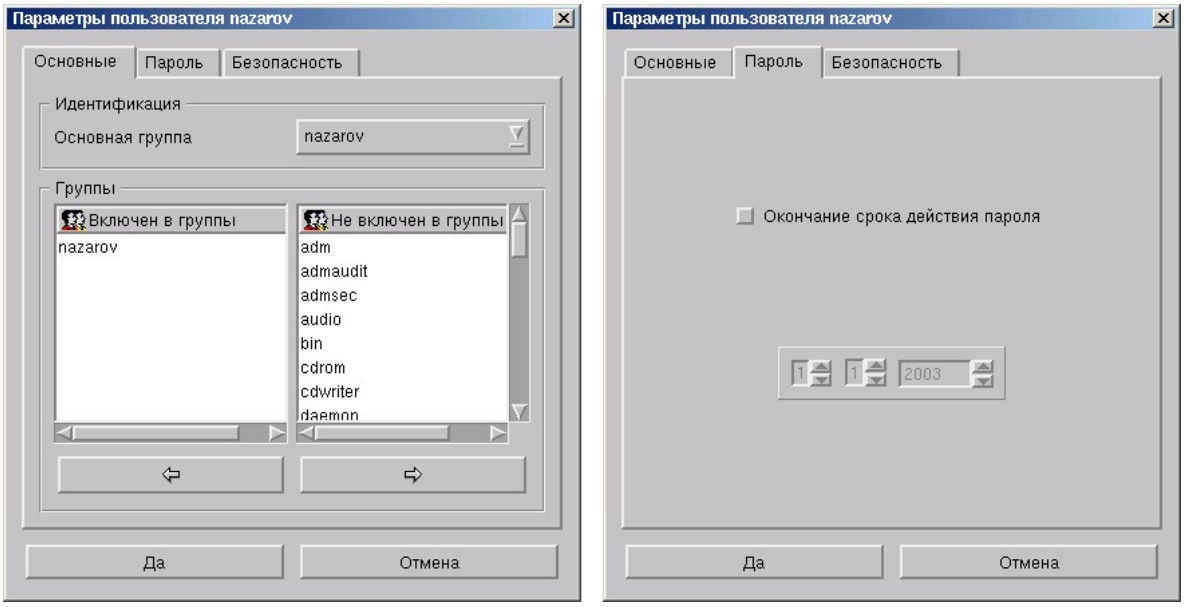


Рис. 18. Диалоговое окно редактирования параметров пользователя

Закладка **«Основные»** позволяет изменить принадлежность пользователя основной и дополнительным группам. В верхней части закладки выбрана основная группа пользователя, которая может быть изменена при помощи выпадающего списка. В нижней части закладки расположены два списка: список групп, в которые пользователь включен и в которые не включен. При помощи элементов управления (кнопок со стрелками "лево", "право") группы могут быть перемещены между этими двумя списками.

Закладка **«Пароль»** позволяет установить ограничение срока действия пароля пользователя. В центре закладки расположен флажок «Ограничить срок действия пароля». Если флажок не установлен, то срок действия пароля пользователя не ограничен. Установка флажка приводит к активизации элементов ввода даты окончания пароля.

Закладка **«Безопасность»** определяет мандатные права доступа пользователя.

Для принятия параметров, определенных при помощи диалогового окна редактирования пользователя необходимо нажать на кнопку **«Да»** в нижней части диалогового окна, для отмены - **«Отмена».**

2. Управление мандатными правами пользователей с помощью ПО РМ АОБИ

Для просмотра и редактирования мандатных прав доступа пользователя, принадлежащего базе пользователей АС, необходимо нажать на кнопку с рисунком **«Пользователи»** в нижней части закладки **«База пользователей»** (рис. 19). В появившемся окне выбрать закладку **«Безопасность».**

Закладка **«Безопасность»** позволяет просматривать и назначать мандатные атрибуты пользователя. В верхней части при помощи выпадающих списков задаются максимальный и минимальный уровни пользователя. В нижней части расположены три списка категорий: общий

список категорий, которым принадлежит пользователь, минимальный набор категорий пользователя и максимальный набор. При помощи элементов управления (кнопки со стрелками **«лево», «право»)** категории могут быть перемещены между общим списком категорий и списками категорий пользователя.

Редактирование конфигурации мандатной модели защиты (набор уровней и категорий) может быть осуществлено стандартными средствами операционной системы ОС МСВС 3.0, например, с помощью команды **«macadmin».**

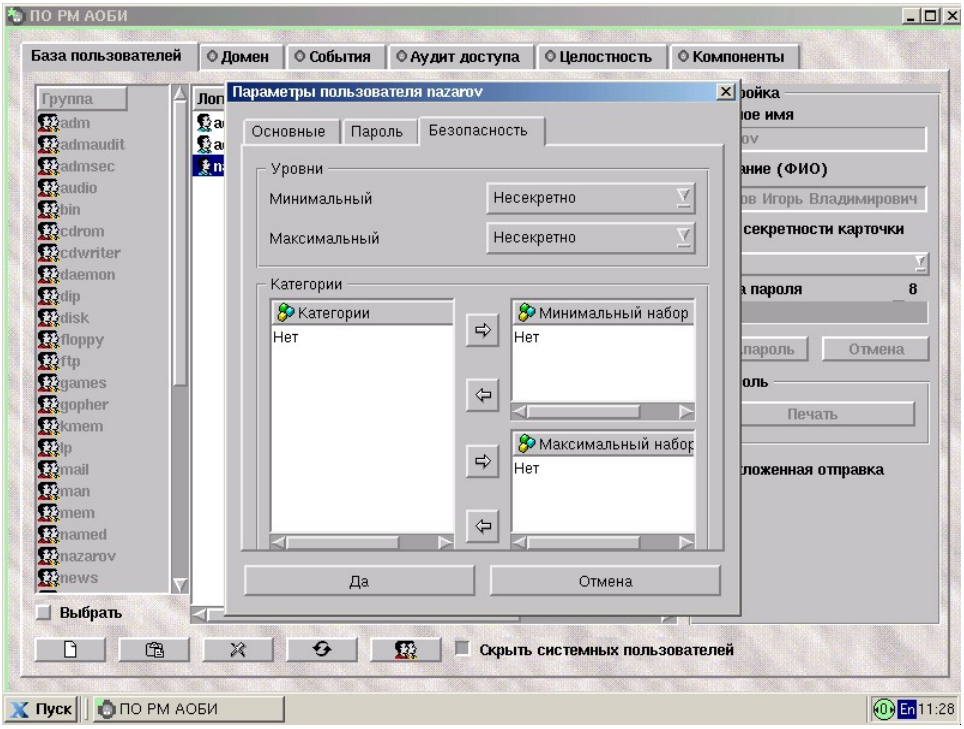


Рис. 19. Диалоговое окно закладки «База пользователей»

Вызов утилиты **macadmin** может быть осуществлен из визуальной системы администрирования АРМ сервера ПО РМ АОБИ. Для этого в закладке **«Домен»** необходимо нажать на кнопку изменения конфигурации мандатной модели (кнопка **«Диаграмма»**, третья слева в нижней части окна). Нажатие кнопки должно привести к вызову программы **macadmin,** интерфейс которой представлен в окне с заголовком **«Категории и уровни»:**

Тиражирование конфигурации мандатной модели защиты подразумевает поддержание на всех АРМ АС одинакового набора уровней и категорий. Эталоном при тиражировании является конфигурация, настроенная на рабочем месте администратора безопасности (АРМ сервера ПО РМ АОБИ).

Для тиражирования конфигурации мандатной модели защиты необходимо перейти в закладку **«Домен»** и нажать на кнопку **«МАС»** (вторая слева в нижней части окна).

После нажатия должно появиться диалоговое окно с запросом подтверждения тиражирования конфигурации мандатной модели защиты. Для отказа от тиражирования файлов конфигурации мандатной модели необходимо нажать на кнопку **«Отмена».** Для подтверждения тиражирования **- «Да».**

Вопрос № 5

«ВКЛЮЧЕНИЕ АРМ КЛИЕНТОВ ПО РМ АОБИ И ПОЛЬЗОВАТЕЛЕЙ В ДОМЕН БЕЗОПАСНОСТИ МСВС 3.0»

Порядок работы:

1. Добавление АРМ АС в домен

В пустом поле, расположенном в правом нижнем углу визуальной среды администрирования ПО РМ АОБИ при выбранной вкладке «Домен», следует ввести IP-адрес клиентского АРМ, либо его символьное имя (при соответствующих настройках в файле **/etc/hosts**).

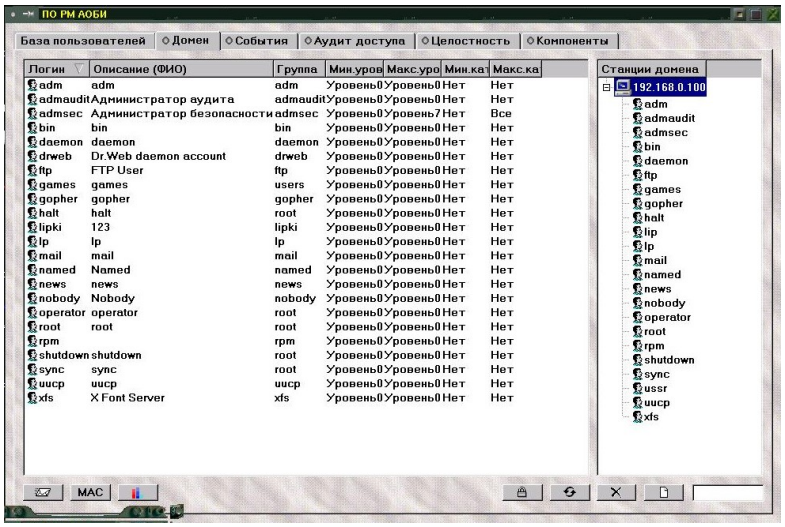
Основные операции с АРМ клиентов ПО РМ АОБИ, включенных в состав домена, можно выполнять, используя четыре кнопки, расположенные слева от поля ввода (рис. 10). Назначение этих кнопок по порядку расположения, слева направо:

- **«Замок»** – разрешение/блокирование входа пользователей на станцию домена;
- **«Стрелки»** – обновление информации о состоянии домена (для получения максимально достоверной информации);
- **«Крест»** – удаление пользователя со станции домена или исключение станции из домена;
- **«Лист»** – включение станции в состав домена.

Для добавления клиентского АРМ в домен следует нажать на кнопку **«Лист».** Пиктограмма АРМ клиента ПО РМ АОБИ появится в поле **«Станции домена».** Рядом с пиктограммой будет указан введенный **IP-адрес** или символьное имя.

Пиктограмма может принимать следующий вид:

- **«Компьютер»** – включенное АРМ клиента ПО РМ АОБИ;
- **«Зачеркнутый компьютер»** – выключенное АРМ клиента ПО РМ АОБИ;
- **«Компьютер на фоне замка»** – заблокированное АРМ клиента ПО РМ АОБИ (вход пользователей невозможен);
- **«Компьютер с глазами»** – АРМ клиента ПО РМ АОБИ, сетевой интерфейс которого находится в режиме прослушивания трафика;



- **«Обесцвеченный компьютер»** – АРМ клиента ПО РМ АОБИ, на котором не запущен агент ПО РМ АОБИ.

Примечание: на каждом добавленном в домен АРМ клиента ПО РМ АОБИ должен быть запущен агент ПО РМ АОБИ.

2. Блокировка АРМ клиента ПО РМ АОБИ

Автоматическое блокирование АРМ клиента ПО РМ АОБИ наступает после троекратной попытки ввода неправильного имени пользователя и (или) пароля. При этом на экране АРМ сервера ПО РМ АОБИ появится следующее сообщение (если запущена визуальная система администрирования сервера ПО РМ АОБИ) (рис. 13):

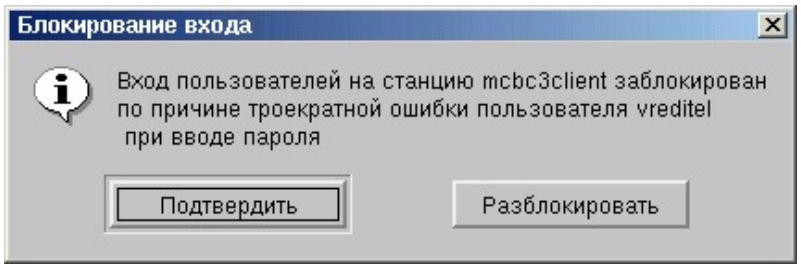


Рис. 13. Диалоговое окно с сообщением о блокировки входа

Суперпользователь сервера ПО РМ АОБИ может отменить или подтвердить блокировку.

Если визуальная система администрирования сервера ПО РМ АОБИ не была запущена, то после ее запуска АРМ клиента ПО РМ АОБИ будет отображаться с пиктограммой **«Компьютер на фоне замка»**. Разблокировать АРМ клиента ПО РМ АОБИ можно, воспользовавшись кнопкой **«Замок».**

С помощью кнопки **«Замок»** суперпользователь сервера ПО РМ АОБИ может в любой момент заблокировать или разблокировать любое АРМ клиента ПО РМ АОБИ.

Ни один пользователь не сможет выполнить процедуру входа в систему на заблокированном АРМ клиента ПО РМ АОБИ, за исключением суперпользователя этого АРМ. Суперпользователь АРМ клиента ПО РМ АОБИ имеет право входа в систему, несмотря на ее блокировку, а также может отменить блокировку АРМ без вмешательства суперпользователя АРМ сервера ПО РМ АОБИ. Для этого он должен удалить файл **/etc/nologin.**

При выполнении блокирования АРМ сеансы всех пользователей этого АРМ будут принудительно завершены.

Таким образом, достигается высокая степень защищенности АРМ клиента ПО РМ АОБИ от действий злоумышленника. С другой стороны, троекратный неправильный ввод пароля легитимным пользователем из-за невнимательности может создать неудобства в работе другим пользователям.

3. Добавление нового пользователя на АРМ сервера ПО РМ АОБИ

Необходимо выбрать закладку **«База пользователей».** Основные операции с пользователями АРМ сервера ПО РМ АОБИ, можно выполнять, используя пять кнопок, расположенных в левом нижнем углу окна. Назначение этих кнопок по порядку расположения, слева направо:

- **«Лист»** – добавление нового пользователя;
- **«Конверт»** – изменение пароля пользователя;
- **«Крест»** – удаление пользователя;
- **«Стрелки»** – обновление внесенных изменений для выбранных пользователей на станциях домена;
- **«Пользователи»** – редактирование параметров пользователя.

Рядом с перечисленными кнопками присутствует флаг с комментарием **«Скрыть системных пользователей»**. После активации этого флага будут отображаться только учетные записи, которые можно использовать для совершения процедуры входа на АРМ. Если указанная **«радио-кнопка»** не нажата, то будет отображаться полный список пользователей, соответствующий содержанию файла **/etc/passwd (**рис. 14**)**.

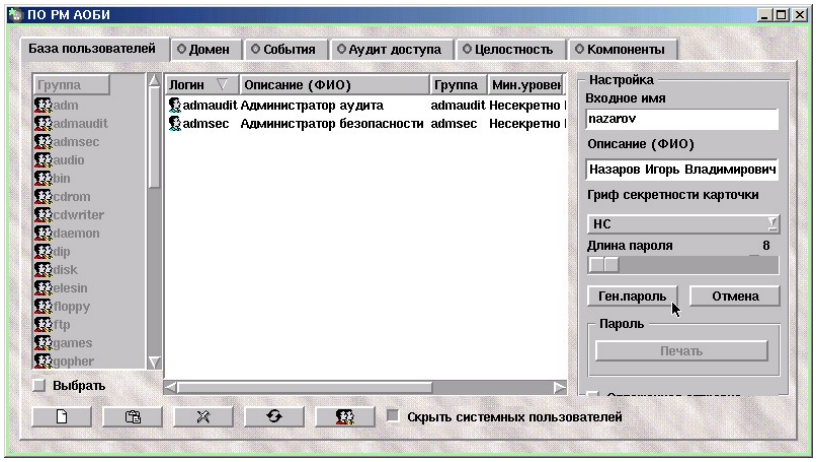


Рис. 14. Диалоговое окно с открытой вкладкой «База пользователей»

Для добавления нового пользователя требуется нажать на кнопку **«Лист».** Эта же операция может быть выполнена при помощи меню, выпадающего при нажатии правой кнопки мыши на списке пользователей. В меню необходимо выбрать пункт **«Добавить».**

Это приведет к активизированию элементов диалога, расположенных в правой части рабочего окна. Необходимо определить следующие параметры для добавляемого пользователя:

- входное имя пользователя **(login);**
- описание или реальное имя пользователя **(ФИО);**
- гриф секретности **(для печати карточек паролей);**
- длину пароля **(от 8 до 16 символов).**

После этого следует нажать на кнопку **«Ген.пароль»** для генерации пароля для данного пользователя. Генерация пароля осуществляется программой генерации паролей, которая была установлена отдельным пакетом **PGP-1.0-3cbit**. Здесь следует вспомнить об ее интеграции в ПО РМ АОБИ. После успешной генерации пароля, единственной активной кнопкой диалога добавления нового пользователя становится кнопка **«Печать».** Остальные кнопки блокируются.

В данный момент учетная запись пользователя добавлена в файл **/etc/passwd**, и в файле **/etc/shadow** определен пароль, соответствующий этой учетной записи и хранящийся в зашифрованном виде. Таким образом, пароль нового пользователя остается никому неизвестен. Для вывода информации о пароле в открытом виде, необходимо нажать на кнопку «Печать», вызвав диалог (рис. 15):

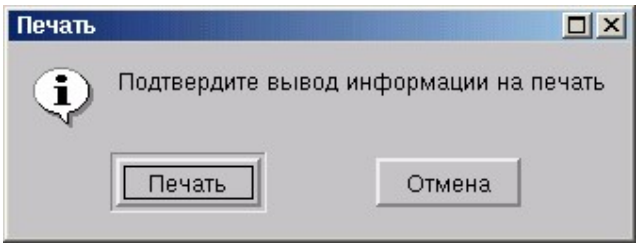


Рис. 15. Диалоговое окно для подтверждения действия

Информация о пароле пользователя может быть выведена только на печать и только однократно. При этом на печать выводится документ с определенными реквизитами, включая

максимальный гриф секретности информации, к которой допущен пользователь. Этот гриф является грифом документа, выведенного на печать и содержащего пароль. Документ должен быть учтен в соответствии с требованиями руководящих документов по секретному (гриф **«секретно»** и выше) или несекретному делопроизводству (гриф **«несекретно»**).

Таким образом, АРМ сервера ПО РМ АОБИ должно быть оборудовано работоспособным принтером, настроенным и готовым к работе. При отказе принтера и крайней необходимости добавить пользователя, можно воспользоваться стандартной командой **«useradd <username>»** и назначить пароль вручную с помощью команды **«passwd <username>»**. Но, как отмечалось выше, на всех АРМ домена должен быть установлен драйвер ограничения полномочий суперпользователя, который не позволяет вносить изменения в файлы **/etc/passwd** и **/etc/shadow** в обход визуальной системы администрирования ПО РМ АОБИ.

Итак, учетные записи пользователей должны добавляться исключительно с помощью визуальной системы администрирования ПО РМ АОБИ, и, следовательно, пароли должны генерироваться и выводиться на печать.

4. Тиражирование пользователя на АРМ клиентов ПО РМ АОБИ

После добавления нового пользователя на АРМ сервера ПО РМ АОБИ, необходимо обеспечить возможность совершения успешной процедуры регистрации данного пользователя на одной или нескольких станциях домена безопасности МСВС 3.0. Для этого требуется создать данному пользователю учетную запись на этих (выбранных) АРМ клиентов ПО РМ АОБИ. Сервер ПО РМ АОБИ способен выполнить эту процедуру автоматически, используя тиражирование данных об учетной записи на станции указанных клиентов ПО РМ АОБИ.

Для выполнения процедуры тиражирования учетной записи пользователя на выбранные АРМ клиентов ПО РМ АОБИ, необходимо выбрать имя этой учетной записи в списке пользователей в закладке **«Домен».** Далее следует выбрать одно, несколько или все АРМ клиентов ПО РМ АОБИ, указанные в поле **«Станции домена»** (эти станции должны быть включены и работоспособны). После этого необходимо нажать на кнопку с изображением письма, расположенную в левом нижнем углу окна. Должно появиться диалоговое окно с запросом подтверждения тиражирования (рис. 16):

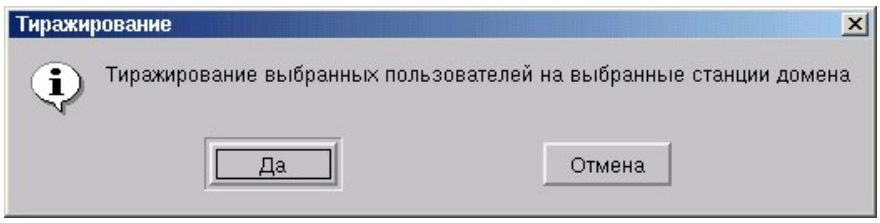


Рис. 16. Диалоговое окно с запросом подтверждения тиражирования

Для отказа от тиражирования необходимо нажать кнопку «Отмена». Для подтверждения тиражирования - «Да».

Разрешается тиражировать несколько учетных записей одновременно. При выполнении операции тиражирования, на выбранных АРМ клиентов ПО РМ АОБИ заводятся учетные записи заданных пользователей, причем сохраняются следующие идентификационные характеристики:

- входное имя пользователя;
- реальное имя пользователя;
- уникальный идентификатор пользователя (uid);
- идентификатор группы (gid);
- имя группы (если такой группы на момент тиражирования нет на АРМ, то она создается);
- пароль;
- мандатные атрибуты пользователя (минимальные и максимальные группы и категории).

5. Изменение пароля пользователя

Изменение пароля пользователя в рамках АС должно быть выполнено только средствами ПО РМ АОБИ. Для этого в закладке **«База пользователей»** необходимо нажать на кнопку изменения пароля (вторая слева в нижней части окна). Аналогичная операция может быть произведена при помощи выпадающего меню, вызываемого нажатием правой кнопки мыши на список пользователей - пункт меню **«Редактировать».**

Изменение пароля может быть применено не только к одному пользователю, но и к целой группе. Для выбора группы можно выделить требуемых пользователей в списке при помощи манипулятора «мышь» или нажатием клавиши «пробел» на соответствующих пользователей.

В правой части окна сделаются доступными элементы диалога для выбора грифа секретности и длины пароля.

Для отказа от изменения пароля необходимо нажать на кнопку **«Отмена»,** для осуществления изменения - **«Применить».** Изменение пароля будет автоматически тиражировано на все АРМ клиентов ПО РМ АОБИ.

Измененные пароли становятся доступны для печати. Печать, так же как и при добавлении пользователя, может быть осуществлена только однократно.

6. Удаление пользователя

Для удаления пользователя из базы пользователей АС необходимо использовать средства ПО РМ АОБИ. В закладке **«База пользователей»** необходимо выбрать в списке требуемое имя учетной записи пользователя для удаления.

После этого необходимо нажать на кнопку удаления **(«Крест»)** в нижней части главного окна. Данная операция может быть также выполнена при помощи выпадающего меню, вызываемого нажатием правой кнопки «мыши» на удаляемого пользователя - пункт меню **«Удалить».** Должно появиться диалоговое окно с запросом подтверждения удаления пользователя с АРМ (рис. 17):

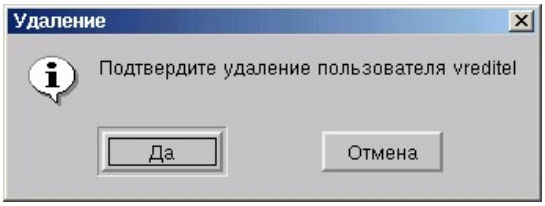


Рис. 17. Диалоговое окно с запросом подтверждения удаления пользователя с АРМ

Для отказа от удаления пользователя необходимо нажать на кнопку **«Отмена».** Для подтверждения удаления - **«Да».**

Удаление пользователя производится на АРМ сервера ПО РМ АОБИ, при этом учетная запись данного пользователя автоматически удаляется со всех АРМ клиентов ПО РМ АОБИ, на которых она была тиражирована.

Помимо операции удаления пользователя из базы пользователей АС, ПО РМ АОБИ предоставляет возможность удаления заданного пользователя с определенного АРМ клиента ПО РМ АОБИ. Для этого необходимо открыть закладку **«Домен».** Выбрать в списке, расположенном в левой части окна, АРМ клиента ПО РМ АОБИ, с которого будет удаляться пользователь. Раскрыть выпадающий список пользователей данного АРМ. В этом списке выбрать пользователя, подлежащего удалению. Нажать на кнопку удаления **«Крест»** в нижней части окна. Должно появиться диалоговое окно с запросом подтверждения удаления пользователя с АРМ. Для отказа от удаления пользователя необходимо нажать на кнопку **«Отмена».** Для подтверждения удаления - **«Да».**

Кроме того, удаление пользователя может быть осуществлено с использованием выпадающего меню. Необходимо навести курсор мыши на удаляемого пользователя и нажать правую кнопку мыши. В выпадающем меню выбрать **«Удаление»,** что приведет к появлению диалогового окна с запросом подтверждения удаления пользователя с АРМ клиента ПО РМ АОБИ.

Удаление учетной записи пользователя с АРМ клиента ПО РМ АОБИ автоматически приводит к завершению сеанса этого пользователя, если такой сеанс (или сеансы) был открыт на момент выполнения операции удаления.

Методические указания

Во вступительной части преподавателю объявить тему, цель учебные вопросы и последовательность проведения занятия, отметить практическую значимость для пользователя ПК знание особенностей инсталляции ОС на ПЭВМ, используемую литературу.

Готовность обучающихся к занятию проверить по наличию у них рекомендованной литературы, рабочих тетрадей с записями, сделанными в них при подготовке к данному практическому занятию, а также в ходе проведения опроса (коллоквиума).

Коллоквиум проводится в письменной форме. По результатам индивидуального опроса преподаватель делает заключение о возможности допуска обучающихся к выполнению занятия. Обучающимся, недостаточно подготовленным к выполнению занятия, дать задание по устранению недостатков и установить время повторного собеседования. Обучающихся, допущенных к выполнению занятия, распределить по рабочим местам, после чего перейти к отработке первого учебного вопроса.

Отработку первого учебного вопроса проводить на компьютерах в соответствии с заданием. В ходе выполнения занятия обучающимися преподавателю контролировать их действия, добиваясь полного выполнения задания. В случае возникновения технических неполадок принимать немедленные меры по приведению компьютера и программного обеспечения в рабочее состояние, привлекая для этого при необходимости, инженера лаборатории. Следить за правильностью и своевременностью выполнения действий, предусмотренных заданием на практическое занятие.

При отработке первого вопроса основное внимание обратить на приобретение обучающимся первоначальных практических навыков в работе с виртуальной машиной. Показать на конкретных примерах работу виртуальной машины.

После окончания выполнения задания обучающиеся выключают компьютеры, оформляют отчеты по работе и представляют их преподавателю для проверки и последующей защиты. Каждый обучающийся оформляет отчет в своей рабочей тетради. Порядок защиты определяется преподавателем; защита может проходить в составе рабочих групп, либо индивидуально каждым обучающимся.

При проверке отчета преподавателю обратить внимание на полноту и качество выполненных записей, таблиц и графических материалов (оформление).

При проверке ответов на контрольные вопросы оценивать краткость, конкретность и правильность ответов.

В ходе проверки отчета обязательно проверять грамотность изложения, все обнаруженные ошибки отмечать и, при необходимости, вносить исправления.

Оценку за выполнение занятия выставить в классный журнал и рабочую тетрадь курсанта, записав, при необходимости, замечания, направленные на улучшение подготовки.

В заключительной части подвести итоги занятия, объявить оценки. Напомнить о необходимости выполнить работу и отчитаться за нее тем, кто по каким-либо причинам отсутствует на данном занятии; установить для этого дату и время. Объявить тему следующего занятия и дать указания на подготовку к нему.

Доцент 27 кафедры
к.т.н.
подполковник

С. Краснов

«___»_____20__г.