ВОЕННО-КОСМИЧЕСКАЯ АКАДЕМИЯ ИМЕНИ А.Ф. МОЖАЙСКОГО

Кафедра № 27 Математического и программного обеспечения

УТВЕРЖДАЮ
Начальник 27 кафедры
полковник_____С.Войцеховский

«___» _____ 201_ г.

Автор: старший преподаватель 27 кафедры
кандидат технических наук
подполковник С.Краснов

Лекция № 18

Тема: «СИСТЕМА ЗАЩИТЫ ОТ НСД ОС МСВС»

по дисциплине: «Защита информации»

Обсуждено и одобрено на заседании 27 кафедры
протокол № __ «____» _____ 2016 г.

Санкт-Петербург
201_

Содержание занятия и время

Введение – 5 мин.

Учебные вопросы (основная часть):

1. Реализация защиты в комплексе «Система защиты от НСД – 30 мин.
2. Команды управления аудитом – 30 мин.
3. Команды управления файлами пользователей и групп пользователей и восстановления файловой системы – 20 мин.

Заключение – 3-5 мин.

Литература:

Основная:

1. Войцеховский С.В., Воробьёв Е.Г. Методы и средства защиты компьютерной информации: учебно-методическое пособие. – СПб.: ВКА имени А.Ф. Можайского 2013. – 134 с.
2. Воробьев Е.Г. Защита информации в автоматизированных системах военного назначения. Учебное пособие – СПб, ВКА им.А.Ф. Можайского, 2007. – 252 с.

Дополнительная:

1. Вихорев С.В. Классификация угроз информационной безопасности. - http://www2.cnews.ru/comments/security/elvis_class.shtml
2. Войцеховский С.В., Марковский А.С., Палагушин В.А. Защита информации в автоматизированных системах. / Под ред. профессора Хомоненко А.Д. – Спб.:НТЦ им. Л.Т. Тучкова, 2005. – 149 с.

Материально техническое обеспечение:

1. Технические средства обучения: ПЭВМ, мультимедиа проектор, экран, программное обеспечение.
2. Приложения (слайды).
3. Наглядные средства обучения – доска, мел.

Организационно-методические указания:

Цель лекции: *Дать знания в области защиты ОС МС ВС.*

Во введении сформулировать тему лекции, цель и название изучаемых вопросов. При этом произвести опрос курсантов по пройденному материалу.

Применяемым методическим приемом является рассказ.

В основной части сконцентрировать внимание курсантов механизмах защиты ОС МС ВС.

В заключительной части обобщить изложенный материал и осуществить контрольный опрос.

1. Перечислите особенности защиты в ОС МС ВС?
2. Охарактеризуйте ОС МС ВС?
3. Перечислите основные задачи администратора безопасности в ОС МС ВС?

Отвечаю на вопросы по теме занятия, даю задание на самостоятельную подготовку.

Лекция № 16

Тема № 5 Механизмы защиты операционных систем

В. 1. Реализация защиты в комплексе «Система защиты от НСД»

В составе СЗИ ОС МСВС 3.0 функционируют следующие механизмы, обеспечивающие разграничение доступа и аудит:

1) мандатное управление доступом (Mandatory Access Control - MAC). Мандатная политика позволяет определять для информации уровни секретности и принадлежность к различным категориям;

2) дискреционное управление доступом (Discretional Access Control - DAC). Каждому файлу ОС МСВС 3.0 сопоставляется список прав доступа (Access Control List - ACL), позволяющий контролировать доступ к данному файлу с точностью до отдельного пользователя системы;

3) аудит. В ОС МСВС 3.0 функционирует система аудита, позволяющая протоколировать события отдельно для каждого пользователя системы. ОС МСВС 3.0 позволяет осуществлять аудит открытия файлов, запуска программ, установку драйверов, входа и выхода пользователей и других событий;

4) привилегии. В ОС МСВС 3.0 функционирует система привилегий (т.н. capabilities), позволяющая отдельным пользователям выполнение различных административных действий.

Мандатное управление доступом

Управление доступом основано на сопоставлении меток безопасности субъекта и объекта.

Субъект может читать информацию из объекта, если уровень секретности субъекта не ниже, чем у объекта, а все категории, перечисленные в метке безопасности объекта, присутствуют в метке субъекта. В таком случае говорят, что метка субъекта доминирует над меткой объекта. Смысл сформулированного правила понятен - читать можно только то, что положено.

В ОС МСВС 3.0 поддерживается до восьми уровней секретности (от 0 до 7, 0 -самый низкий, 7 - самый высокий) и до 61 различной категории. Каждому уровню или категории назначается соответствующее имя и значение с помощью программы macadmin. Например, система может быть настроена на работу с тремя уровнями секретности: "Несекретно", "Секретно", "Совершенно секретно".

Дискреционное управление доступом

Список прав доступа содержит основные (владелец, владелец-группа, остальные) и расширенные атрибуты доступа. Расширенные атрибуты определяют права доступа к файлу для отдельного пользователя или отдельной группы пользователей.

Полномочия на файл или каталог, можно узнать с помощью команды «Ls», введенной с ключом «-L» и именем файла (либо полным путем к нему), указанным в качестве аргумента, как показано в следующем примере:

[root@mcbc3server /root]# ls -l readme\ -\ text

- r-x r-x r-x 1 root root 4057784 Фев 6 18:53 readme – text

В приведенном примере получен список полномочий на текстовый файл.

Полученный результат содержит в начале строки запись -r-xr-xr-x. Эту запись следует разобрать подробно, а для наглядности она разделена по колонкам таблицы, как показано ниже:

Тип файла	Права доступа	Права доступа	Права доступа

	владельца файла (в примере – **root**)	группы файла (в примере – **root**)	всех остальных пользователей
-	**r-x**	**r-x**	**r-x**

Типы файлов могут принимать следующие значения:

–	–	обычный файл			
d	–	каталог	**l**	–	символьная ссылка
b	–	блочное устройство	**p**	–	FIFO
c	–	символьное устройство	**s**	–	гнездо (socket)

Права доступа делятся на чтение (read, обозначается буквой r), запись (write, обозначается буквой w) и исполнение (execute, обозначается буквой x). Как видно из таблицы, в каждом столбце указывается совокупность прав доступа. Для объяснения полномочий прав доступа используется восьмеричная система счисления, где каждому из прав соответствует свое **восьмеричное** число: r – 4, w – 2, x – 1. Представленная ниже таблица 8.1 поясняет систему назначения прав в целом и показывает все возможные комбинации прав доступа.

Табл. 8.1.

Возможные комбинации прав доступа

4 (r)	**2 (w)**	**1 (x)**	Расчет	Сумма	Абрев.	Наличие прав доступа
0	0	0	0 + 0 + 0	0	---	права доступа отсутствуют
0	0	1	0 + 0 + 1	1	--x	только исполнение
0	1	0	0 + 2 + 0	2	-w-	только запись
0	1	1	0 + 2 + 1	3	-wx	запись и исполнение
1	0	0	4 + 0 + 0	4	r--	только чтение
1	0	1	4 + 0 + 1	5	r-x	чтение и исполнение
1	1	0	4 + 2 + 0	6	rw-	чтение и запись
1	1	1	4 + 2 + 1	7	rwx	чтение, запись и исполнение

Помимо основных прав доступа (r, w, x) существуют дополнительные права доступа.
Права доступа назначаются с помощью команды «chmod», например:

```
[root@mcbc3server /]# chmod 0644 file.txt
[root@mcbc3server /]# ls -l file.txt
-rw-r--r--    1 root  root      1 Фев 24 22:17 /restore/target
```

Команда chmod с ключом «-R» применяется при назначении прав доступа каталогу.

В назначении прав доступа существуют правила, указанные в табл. 8.2, 8.3, которых следует придерживаться:

Табл. 8.2.

Рекомендации для файлов

Тип файла	**Уровень полномочий**	
	Владелец файла	Пользователь файла
Исполняемый файл	**7** (rwx)	**5** (r-x)
Файл документа	**6** (rw-)	**4** (r--)

1 (**--x**) – нельзя запрещать чтение исполняемых файлов.

2 (**-w-**) – отсутствие разрешения r при наличии разрешения w, как правило, приводит к ошибкам. Например, при попытке открыть такой файл встроенным редактором Midnight Commander вся информация в файле уничтожается.

3 (**-wx**) – внесение изменений в исполняемый файл может привести не только к неработоспособности программы, но и создает угрозу безопасности системы: злоумышленник может подменить исполняемый файл троянской программой.

По-другому выглядят рекомендации для каталогов.

Табл. 8.3.

Рекомендации для каталогов

Тип файла	Уровень полномочий	
	Владелец файла	Пользователь файла
Каталог	**7** (rwx)	**5** (r-x)

Разрешение «x» позволяет открыть каталог, а разрешение «r» – просмотреть его содержимое. По отдельности разрешения «x» и «r» смысла не имеют, но в совокупности обеспечивают минимально необходимый для работы уровень доступа. Пользователь не может удалять и создавать файлы в этом каталоге.

Система аудита

Система аудита ОС МСВС 3.0 позволяет осуществлять протоколирование следующих событий: Для файлов:

- запуск файла на исполнение;
- открытие файла;
- удаление файла;
- изменение мандатных атрибутов файла;
- изменение флагов протоколирования файла.

Для процессов:

- запуск программ на исполнение;
- открытие файлов;
- удаление файлов;
- изменение списка прав доступа файлов;
- изменение мандатных меток файлов и процессов;
- изменение привилегий процессов;
- загрузку и выгрузку драйверов;
- монтирование и размонтирование файловых систем;
- изменение дискреционных атрибутов процессов;
- изменение политики аудита.

Система аудита ОС МСВС 3.0 обеспечивает доверенность аудита, т.е. невозможность подделать или скрыть событие аудита, или получить несанкционированный доступ к журналам аудита.

Аудит событий настраивается отдельно для каждого пользователя или группы пользователей.

Аудит событий файловой системы (запуск программы на исполнение и открытие файла) и аудит процессов пользователей (групп) функционируют независимо. Например, можно установить аудит запуска программы /bin/su и аудит открытия файла /etc/shadow. Отдельно можно установить аудит запуска всех программ и/или открытия файлов для некоторых пользователей (групп).

Для настройки и управления системой аудита в ОС МСВС 3.0 предусмотрен специальный администратор аудита. Его функции может также выполнять привилегированный пользователь.

Система привилегий

Система привилегий ОС МСВС 3.0 предназначена для передачи отдельным пользователям выполнения различных административных действий. Обычный пользователь системы не имеет дополнительных привилегий.

Пользователь, обладающий дополнительными привилегиями, называется системным администратором, а набор действий, которые он может выполнять называется его ролью. В ОС МСВС 3.0 на данный момент имеется два предустановленных системных

администратора - администратор безопасности (входное имя admsec) и администратор аудита (входное имя admaudit). Привилегированный пользователь имеет идентификатор равный нулю. Независимо от кода защиты файла привилегированный процесс имеет право доступа к файлу для чтения и записи.

Назначение привилегий обычным пользователям ЗАПРЕЩЕНО.

Администратор безопасности:

- полностью игнорирует мандатную политику, в том числе при сетевом взаимодействии;
- может изменять мандатные метки и мандатные атрибуты файлов (каталогов);
- может назначать и изменять мандатные метки пользователей;
- может настраивать мандатную политику, т.е. определять количество уровней и категорий в системе, их имена и значения.

Администратор аудита:

- может устанавливать аудит на объекты файловой системы (запуск файла на исполнение, открытие файла и т.д.);
- может устанавливать аудит для пользователей (групп) системы (например, для некоторого пользователя можно установить аудит запуска всех программ);
- может устанавливать политику аудита по умолчанию (для пользователей/групп, не указанных специально);
- может настраивать систему аудита. Данная возможность имеет ограничение: администратор аудита может ввести изменения в действие только после перезагрузки системы (не может перезапустить систему аудита);
- может настраивать службу аудита для обеспечения доверенности аудита;
- может просматривать и обнулять журналы аудита.

Для построения защищенной автоматизированной системы на базе МСВС 3.0 с возможностью временной совместимости с NT была разработана **система терминального доступа**. Данная система позволяет организовать в МСВС работу с Windows-приложениями следующим образом: серверы файлов и печати, а также клиентские места строятся на базе МСВС 3.0, а для работы с Windows-приложениями выделяется сервер приложений на базе NT Terminal Server Edition, доступ к которому осуществляется специальным образом.

Одно из **достоинств** данного варианта — это гибкость в организации работы пользователей, которые фактически получают возможность работать одновременно в двух операционных средах и использовать приложения каждой из них.

Недостаток — необходимость создания сервера приложений со специальным доступом, что приводит к появлению ограничений в политике безопасности. В результате, задача интеграции МСВС и Windows NT решается путем создания домена МСВС с сервером приложений на базе NT и использования системы терминального доступа.

Рассмотрим, как работает пользователь в гетерогенном домене МСВС. Пользователь входит в домен через свой АРМ. Для обращения к серверу приложений на базе Windows NT пользователь обращается к клиенту терминального доступа. В специальной базе данных, хранящейся на сервере приложений, имеется соответствие между именем пользователя и именем его компьютера, которое используется при подключении сетевых дисков для данного пользователя. В результате, работая в сеансе NT, пользователь в качестве сетевого диска на своем рабочем месте видит только содержимое своего домашнего каталога, а также общие ресурсы домена (файловые серверы и принтеры). Он может запускать приложения Windows, но будет работать только с ограниченным множеством файлов (своих или общих), хранящихся на компьютерах с МСВС 3.0.

Для организации печати конфиденциальных документов в домене выделяется сервер печати на базе МСВС, который отвечает за осуществление и учет печати, что предотвращает безучетное размножение выходных конфиденциальных документов. Для печати не конфиденциальной информации возможно подключение локальных принтеров к АРМ. Пользователь, работая с приложениями Windows или МСВС, посылает документ на

печать, причем не имеет значения, где находится документ — на локальной машине или на сервере файлов. С помощью средств МСВС происходит анализ уровня конфиденциальности документа. Если документ является конфиденциальным, задание перенаправляется на сервер печати, если нет, — документ печатается локально.

ЗАЩИТА ХРАНИМЫХ ДАННЫХ

Для защиты хранимых данных в составе ОС МСВС 3.0 имеется утилита crypt, которая читает данные со стандартного ввода, шифрует их и направляет на стандартный вывод.

Шифрование применяется при необходимости предоставления абсолютного права владения файлом. Зашифрованный файл можно прочитать лишь по предъявлении пароля.

В. 2 Команды управления аудитом

Команда **auditadmin**

Команда auditadmin предназначена для настройки журнапирования, протоколирования и доверенности системы аудита из графической оболочки.

Журналирование - распределение сообщений о событиях аудита по журналам. В зависимости от типа и важности события администратор может назначить соответствующий журнал для его записи.

Протоколирование - фиксация системой заданного набора событий, для пользователя/группы. Администратор может назначить для пользователей/групп различные наборы событий, которые будут фиксироваться в журналах аудита.

Доверенность - невозможность подделать или скрыть событие аудита. Администратор может запретить/разрешить для различных пользователей фиксацию событий различных типов и важности. При запрете фиксации некоторого события, если это событие происходит, вместо фиксации события в журнал выдается предупреждение.

5.6.2. Команда **chaudit**

Команда chaudit предназначена для назначения протоколирования событий для файлов ОС МСВС 3.0. Программа chaudit выполняется из командной строки и позволяет назначить или снять с файла(ов) протоколирования следующих событий:

- запуск файла на исполнение;
- открытие файла;
- удаление файла;
- изменение мандатных атрибутов файла;
- изменение флагов протоколирования файла.

Синтаксис команды:

chaudit [ОПЦИИ] ... ВЕКТОР_ФЛАГОВ_АУДИТА ФАЙЛ.

Описание команды и опций:

Команда chaudit изменяет флаги аудита для каждого ФАЙЛА на указанные в ВЕКТОР_ФЛАГОВ_АУДИТА. Опции команды chaudit:

-f, -silent, -quiet –	не выводить сообщения об ошибках.
-v, -verbose –	выводить диагностические сообщения для каждого файла.
-c, -changes –	то же, что и -verbose, но сообщать только об изменениях.
-R, -recursive –	применить рекурсивно,
-h, -help –	вывести справку и выйти,
-version	вывести информацию о версии и выйти.

ВЕКТОР_ФЛАГОВ_АУДИТА - это комбинация следующих символов:

o -	установить аудит на открытие файла;
x -	установить аудит на выполнение файла;
d -	установить аудит на удаление файла;

m - установить аудит на изменение мандатных свойств файла;
O - снять аудит на открытие файла;
X - снять аудит на выполнение файла;
D - снять аудит на удаление файла;
M - снять аудит на изменение мандатных свойств файла;
A - снять аудит на изменение флагов аудита.

ВЕКТОР_ФЛАГОВ_АУДИТА может быть также задан в виде шестнадцатеричного числа.

5.6.3. Команда **logwatch**

Команда logwatch предназначена для выборочного ознакомления с журналами аудита. Она позволяет производить выборку и обобщение информации по событиям аудита в соответствии со следующими критериями:

- тип события;
- дата события;
- субъект доступа (пользователь);
- тип доступа (открытие файла, запуск программы, изменение свойств файла и т.д.);
- объект доступа (файла);
- результат доступа (успешно/неуспешно осуществлен доступ).

Синтаксис команды:

logwatch /usr/sbin/logwatch [--detail <level>] [-logfile <name>]
[-print] [-mailto <addr>] [-archives] [-range <range>] [-option <name=value>]
- [-debug <level>] [-save <filename>] [-help] [-version] [-service <name>]

B. 3 Команды управления файлами пользователей и групп пользователей и восстановления файловой системы

Команды управления файлами пользователей и групп пользователей (/etc/passwd и /etc/group, соответственно) предназначены для прямого редактирования соответствующих файлов с помощью редактора Vi, а также проверки корректности записей этих файлов. Системному администратору следует избегать использование этих команд, так как они оставлены для обратной совместимости.

Команда **grpck**

Команда grpck предназначена для проверки целостности файла группы в ОС МСВС 3.0.

Синтаксис команды:

grpck [-r] [group shadow]

Описание команды и опций:

Команда grpck проверяет целостность системной идентификационной информации. Все записи в файлах /etc/group и /etc/gshadow проверяются на надлежащий формат и правильные данные в каждом поле. Пользователь получает приглашение удалить записи, которые имеют не надлежащий формат или которые имеют другие некорректируемые ошибки.

- правильный список членов и администраторов.

Если запись имеет неверный номер поля, то пользователю предлагается удалить данную строку. Если пользователь не отвечает утвердительно, то все следующие записи будут пропущены. Запись с повторяющимся именем группы будет предложено удалить, но все оставшиеся записи будут проверены. Обо всех других ошибках выдается предупреждающее сообщение, и пользователю предлагается запустить команду groupmod для того, чтобы

исправить ошибки. Команды, которые управляют файлом /etc/group, становятся недоступными, после того как файл /etc/group был поврежден.

По умолчанию grpck управляет файлами /etc/group и /etc/gshadow. Но пользователь может выбрать альтернативные параметры group и shadow.

-r – Выполнять команду в режиме только для чтения.

5.8.2. Команда **pwck**

Команда pwck предназначена для проверки целостности файла паролей ОС МСВС 3.0.

Синтаксис команды:

pwck [-r] [passwd shadow]

Описание команды и опций:

Команда pwck проверяет целостность системной идентификационной информации. Все записи в файлах /etc/passwd и /etc/shadow проверяются на надлежащий формат и правильные данные в каждом поле. Пользователь получает приглашение удалить записи, которые имеют не надлежащий формат или которые имеют другие некорректируемые ошибки.

Проверяются:

- корректный номер полей;
- уникальное имя пользователя;
- допустимый идентификатор группы и пользователя;
- допустимая первичная группа;
- допустимая домашняя директория;
- допустимая входная командная оболочка.

Если запись имеет неправильный номер полей, пользователю будет предложено удалить эту строку. Если пользователь не отвечает утвердительно, то все последующие проверки записей будут пропущены. Запись с повторяющимся именем будет предложено удалить, но все оставшиеся записи будут проверены. Обо всех других ошибках выдается предупреждающее сообщение и пользователю предлагается запустить команду usermod для того, чтобы исправить ошибки. Команды, которые управляют файлом /etc/passwd, становятся недоступными, после того как файл /etc/passwd был поврежден.

По умолчанию pwck управляет файлами /etc/passwd и /etc/shadow. Но пользователь может выбрать альтернативные параметры passwd и shadow.

-r – Выполнять команду в режиме только для чтения.

5.8.3. Команды **vipw** и **vigr**

Команды vipw и vigr предназначены для прямого редактирования файлов пользователей и групп пользователей ОС МСВС 3.0.

Синтаксис команд:

vipw [-V] [-version]

vigr *[-V]* [—version]

Описание команд:

Команды vipw и vigr редактируют файлы пользователей и групп пользователей, соответственно, после установки необходимых блокировок. Эти команды редактируют файлы, только если они не редактируются другим пользователем. Если какой-либо из файлов уже заблокирован для редактирования другим пользователем, то вас попросят повторить данную операцию позже. По умолчанию редактором для vipw и vigr является редактор vi.

ВОССТАНОВЛЕНИЕ ФАЙЛОВОЙ СИСТЕМЫ

ОС МСВС 3.0 поддерживает два основных набора утилит копирования: программы **dump/restor и cpio.** Программа **volcopy** целиком переписывает файловую систему, проверяя

с помощью программы **labelit** соответствие меток требуемых томов. Программа **dump** обеспечивает копирование лишь тех файлов, которые были записаны позднее определенной даты (защита накоплением). Программа **restor** может анализировать данные, созданные программой **dump**, и восстанавливать отдельные файлы или всю файловую систему полностью. Программа **cpio** предназначена для создания одного большого файла, содержащего образ всей файловой системы или какой-либо ее части.

Для восстановления поврежденной, например, в результате сбоев в работе аппаратуры, файловой системы используются программа **fsck**. Сначала проверьте корневой каталог командой ***fsck /*** , если обнаружатся какие-либо проблемы, перезагрузите систему. Повторяйте этот процесс до тех пор, пока корневой раздел не будет чист. Потом с помощью команды fsck проверьте остальные файловые системы. Повторяйте ввод команды fsck до тех пор, пока система не загрузится без ошибок.

Не допускается завершение работы пользователей ОС МСВС 3.0 путем выключения питания, нажатия кнопки <Сброс> (<Reset>).

При эксплуатации ОС МСВС 3.0 **запрещается:**

1. использования протокола telnet для работы в автоматизированных системах, имеющих выход за пределы контролируемой зоны;
2. использования файловых систем, отличных от ext2, на автоматизированных рабочих местах и серверах.

Старший преподаватель 27 кафедры
подполковник

С.Краснов