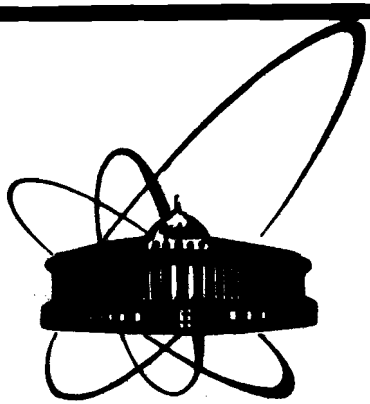

сообщения
объединенного
института
ядерных
исследований
дубна

Р11-88-314

А.Д.Бавижев, В.В.Кореньков

ЗАЩИТА ФАЙЛОВ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА В ОС ЕС

1988

Обеспечение высоконадежных средств защиты информации является одной из основных задач при разработке любой файловой системы.

Хорошая файловая система должна обеспечивать, с одной стороны, возможность совместного использования одних и тех же файлов различными пользователями, а с другой стороны, защиту файлов от несанкционированного доступа.

Стандартная операционная система ОС ЕС имеет в своем составе механизм защиты файлов. Большим недостатком этого механизма является то, что при каждом открытии защищенного набора данных на консоль оператора ЭВМ выдается запрос на ввод соответствующего пароля. Это замедляет процесс прохождения задач в системе, а также предполагает, что оператор ЭВМ должен знать пароли всех защищенных пользовательских файлов. Эти обстоятельства делают крайне неудобным для практического использования существующий в ОС ЕС механизм защиты информации.

Целью данной работы является описание организации и функционирования собственного аппарата защиты файлов от несанкционированного доступа в ОС ЕС с точки зрения пользователя и системного программиста.

Защита файлов обеспечивает:

- контроль санкционированного доступа к файлу до его предоставления;
- прекращение выполнения задания после отказа в доступе;
- регистрацию всех незаконных попыток получения доступа к файлу.

Защита файлов разработана и реализована в рамках стандартной файловой системы ОС ЕС и предназначена для наборов данных, находящихся на магнитных дисках.

I. УПРАВЛЕНИЕ ДОСТУПОМ ДЛЯ ЗАДАЧ ПАКЕТНОЙ ОБРАБОТКИ

Механизм защиты файлов взаимодействует с системой парольного учета пользователей. Поэтому приведем краткое описание системы парольного учета[1].

Задание в операционной системе ОС ЕС идентифицируется по управляющей карте JOB именем задания, полем учетной информации, именем программиста. Система парольного учета идентифицирует по этим данным пользователя, однозначно определяет его принадлежность к конкретному структурному подразделению, тематический план его работы и др.

В ЛВТА ОИЯИ на базовой ЭВМ ЕС-1061 были выбраны следующие принципы организации парольного учета пользователей:

- поле учетной информации в карте JOB содержит текст, первые 5 символов которого являются личным паролем пользователя ЭВМ, обеспечивающим доступ к средствам операционной системы и ЭВМ;
- первый символ пароля определяет подразделение пользователя;
- информация о всех зарегистрированных пользователях хранится в файле паролей. Каждая запись файла паролей содержит пароль пользователя, шифр темы (темы объединяют пользователей, работающих над общими задачами), фамилию и телефон пользователя и др. При загрузке операционной системы в оперативную память ЭВМ (в поле данных резидентного модуля SYSCVT) считываются имена паролей и тем;
- анализ паролей по данным управляющей карты JOB и модуля SYSCVT выполняется программой выхода IEFUJV .

Файловая система ОС ЕС различает два типа доступа к файлам: чтение из файла и запись в файл.

Механизм защиты файлов обеспечивает санкционированность обращения к файлу по каждому из этих типов доступа.

По отношению к любому файлу аппарат защиты файлов помимо упомянутых типов доступа различает три категории пользователей, каждая из которых имеет свои собственные ограничения по любому из типов доступа к файлу. Этими категориями являются: ВЛАДЕЛЕЦ (владелец файла), ЧЛЕНЫ ГРУППЫ (члены группы, к которой принадлежит владелец файла) и ПРОЧИЕ ПОЛЬЗОВАТЕЛИ (все остальные пользователи). Групповое владение файлами позволяет обеспечить каждому члену группы, работающей над общими задачами, возможность осуществлять доступ к файлам других членов этой группы.

Защита файлов организуется на уровне паролей. Каждому защищаемому набору данных присваивается пароль и режим доступа. Пароль в закодированной форме и байт режима доступа заносятся в резервные поля метки файла DSCB1 . Метка DSCB1 содержит основную информацию о файле и располагается в оглавлении тома. Подробную информацию об организации оглавления тома можно найти в работе[2].

Введение файла под парольную защиту осуществляется процедурой PROTECT (см. ниже). Пользователь, защитивший файл от несанкционированного доступа с помощью процедуры PROTECT , считается ВЛАДЕЛЬЦЕМ. ВЛАДЕЛЕЦ может менять пароль и режим доступа к файлу.

Во все время работы с защищенным набором данных действует механизм проверки правильности обращения к защищенному набору. При открытии защищенного набора данных механизм защиты файлов выполняет следующие действия: проверяется, является ли пользователь обрабатывающей программы ВЛАДЕЛЬЦЕМ защищенного файла, путем сравнения личного пароля из карты JOB и пароля из DCSB1 . В случае совпадения доступ к файлу разрешается. В противном случае проверяется, являются ли членами одной группы ВЛАДЕЛЕЦ файла и пользователь обрабатывающей программы, путем сравнения соответствующих элементов таблицы в модуле SYSCVT . В случае совпадения, а также соответствия режима обработки, запрашиваемого в обрабатывающей программе, и режима доступа к файлу в DSCB1 доступ к файлу предоставляется. Если и это условие не выполняется, то на консоль оператора выдается запрос на ввод пароля владельца файла, и если пароль сообщен правильно с двух попыток, то доступ к защищенному файлу разрешается. В противном случае обрабатывающая программа заканчивается аварийно с соответствующим кодом завершения.

Механизм защиты файлов генерирует запись типа 254 и записывает в статистический набор данных системной мониторной программы в случае, когда доступ к защищенному файлу был разрешен, лишь после указания пароля владельца файла с консоли оператора. Запись типа 254 содержит информацию о задаче, получившей доступ к защищенному файлу (имя задания, личный пароль пользователя, дату и время доступа, имя файла, режим доступа и др.).

2. УПРАВЛЕНИЕ ДОСТУПОМ В СИСТЕМЕ TERM

В настоящее время в ЛВТА ОИЯИ на ЕС-1061 эксплуатируется диалоговая система TERM , предназначенная для облегчения доступа пользователей к ЭВМ и средствам операционной системы с помощью терминалов[3]. Система TERM предоставляет пользователям возможность работы с личными наборами данных, совместимыми с наборами операционной системы.

Перед тем как предоставить доступ к защищенному файлу система TERM , пользуясь услугами механизма защиты файлов, проверяет санкционированность такого доступа. При этом механизм защиты файлов идентифицирует пользователя по паролю, введенному при входе в сеанс терминальной работы, а режим доступа определяется типом исполняемой команды (чтение или модификация). Алгоритм предоставления доступа к защищенному файлу в системе TERM такой же, как и при выполнении пакетных задач.

3. ВКЛЮЧЕНИЕ В СИСТЕМУ

Модуль, обеспечивающий защиту файлов от несанкционированного доступа, включается в состав ОС ЕС и вызывается из системных модулей: IFG0196W (модуль программы открытия файлов), IGG0290A (модуль программы удаления файлов), IGG03001 (модуль программы переименования файлов). Модуль защиты файлов получает управление при каждом открытии, удалении и переименовании любого дискового файла.

4. ПРОЦЕДУРА PROTECT

Для обеспечения парольной защиты файлов используется одна процедура PROTECT .

Процедура PROTECT предназначена для:

- введения файла под парольную защиту, снятия защиты с защищенного файла или изменения режимов доступа к файлу;
- изменения пароля;
- получения информации о режимах доступа к защищенному файлу.

Процедуру можно запускать по команде оператора START с консоли, в карте EXEC языка управления заданиями и по терминальной команде ("пульт" в диалоговой системе TERM).

Параметры процедуры:

DS - имя файла; любое имя, допустимое в ОС ЕС.

PWD - пароль доступа к файлу; от I до 5 символов. Если PWD не задан, то процедура PROTECT выполняет функцию получения информации о режимах доступа к защищенному файлу.

U - режим доступа к файлу для всех пользователей; U=R - разрешение на чтение файла, но запрет на запись; U=RW или U=WR - разрешение на запись и на чтение (означает снятие защиты с файла).

G - режим доступа к файлу для членов группы; G=R - разрешение на чтение файла, но запрет на запись; G=RW или G=WR - разрешение на запись и на чтение.

По умолчанию параметры U и G имеют пустое значение (U=,G=), означающее запрет доступа к файлу по записи и по чтению.

OC - выходной класс сообщений; по умолчанию OC=A .

V - имя диска, где расположен файл DS . Для каталогизированного файла можно не задавать.

NPWD - новый пароль доступа к файлу; задается при выполнении функции замены пароля.

ПРИМЕРЫ

I. Введение файла под парольную защиту

```
// EXEC PROTECT,DS='USR.LIB1',PWD=XXXXX,U=R
```

Набору данных USR . LIB1 присвоен пароль XXXXX . Разрешен доступ к файлу по чтению, но запрещен по записи для всех пользователей.

```
// EXEC PROTECT,DS='USR.LIB2',PWD=XXXXX,G=R
```

Набору данных USR . LIB2 присвоен пароль XXXXX . Разрешен доступ к файлу по чтению, но запрещен по записи для членов группы. Для всех пользователей запрещен любой доступ к файлу.

```
// EXEC PROTECT,DS='USR.LIB3'PWD=XX
```

Набору данных USR . LIB3 присвоен пароль XX . Запрещен доступ к файлу по записи и по чтению для всех пользователей и членов группы.

2. Изменение режимов доступа к файлу

```
P S PROTECT, DS='USR.LIB1',PWD=XXXXX,U=R,G=RW,OC=C
```

Всем пользователям обеспечивается доступ к файлу по чтению, а членам группы - по чтению и записи.

3. Снятие защиты с файла

```
// EXEC PROTECT, DS='USR.LIB1',PWD=XXXXX,U=RW
```

Устанавливается режим доступа по записи и чтению для всех пользователей - это означает снятие защиты.

4. Изменение пароля

```
// EXEC PROTECT, DS='USR.LIB2',PWD=XXXXX,NPWD=YYY
```

Пароль доступа XXXXX к защищенному файлу USR . LIB2 изменен на YYY . Режим доступа не изменен. Для смены режима доступа к файлу необходимо задать параметры U и G .

5. Получение информации о режимах доступа

```
P S PROTECT,DS='USR.LIB2',OC=C
```

Выдается информация о режимах доступа к файлу USR.LIB2 . Критерием выбора этой функции является то, что не задан параметр PWD .

Замечания

I. При изменении режимов доступа (пр.2), снятии защиты (пр.3) и смене пароля (пр.4) значение параметра PWD, заданное в процедуре PROTECT, должно совпадать с паролем доступа к файлу, так как предполагается, что файл защищен.

2. Пользователь может работать со своим файлом, не замечая "присутствия" механизма защиты файлов, если в качестве пароля доступа к файлу используется личный пароль пользователя ЭВМ. Это справедливо как для пакетных задач, так и при работе в системе TERM. Однако в некоторых случаях предпочтительнее (с точки зрения секретности) защищать файлы уникальными именами, не совпадающими с личными паролями пользователей ЭВМ.

Например, можно защищать от записи уникальными паролями:

- наборы данных, которые редактируются лишь средствами системы TERM . В этом случае доступ к защищенным файлам предоставляется вводом пароля с экрана терминала;
- редко редактируемые в пакетном режиме наборы данных. В этом случае до выполнения программы редактирования защищенного набора данных необходимо выполнить процедуру PROTECT, выполняющую функцию замены пароля на личный пароль пользователя ЭВМ. Перед завершением задания можно исполнить процедуру PROTECT для обратной смены пароля.

3. На ЕС-1061 в ОИЯИ под группой понимается коллектив пользователей, работающий над одним тематическим планом.

5. СООБЩЕНИЯ

1. Выполнение процедуры PROTECT сопровождается выдачей в выходной класс подробных сообщений на русском языке.

2. Запрос на ввод пароля владельца файла осуществляется с помощью макрокоманды WTOR . На консоль оператора выдается сообщение:

```
*N SECURITY JOB=JJJ DSN=DDD ,
```

N – номер запроса;
JJJ – имя задания;
DDD – имя защищенного файла.

Оператору предоставляются две попытки для введения правильного пароля.

3. Отказ в доступе к защищенному набору данных из программы открытия файлов сопровождается выдачей следующего сообщения:

```
IEC143I 213-08, JJJ, SSS, DDN, DDD, SER, DSN
```

JJJ – имя задания;
SSS – имя пункта задания;
DDN – имя оператора DD для набора данных DSN;
DDD – адрес устройства;
SER – регистрационный номер тома;
DSN – имя набора данных.

4. Незаконная попытка стереть или переименовать защищенный набор данных сопровождается выдачей в листинг программы системного сообщения с префиксом IEH207I , в котором присутствует строка:

```
CORRECT PASSWORD NOT AVAILABLE .
```

5. Система TERM предоставляет пользователю две попытки введения пароля защищенного файла. Пароль вводится после выдачи на экран терминала следующего сообщения:

```
IMPROPER PASSWORD PRESENTED . ENTER PASSWORD .
```

Если обе попытки были безуспешны, то доступ к файлу не предоставляется и выдается сообщение

```
FILE PROTECTED .
```

В заключение авторы считают своим приятным долгом поблагодарить В.П.Ширикова за полезные обсуждения и проявленный интерес к работе.

ЛИТЕРАТУРА

1. Галактионов В.В., Хаиндрава М.Н. ОИЯИ, Р10-82-316, Дубна, 1982.
2. Хусаинов Б.С. Программирование ввода-вывода в ОС ЕС ЭВМ на языке Ассемблера. "Статистика", М., 1980.
3. Кореньков В.В. ОИЯИ, Р11-82-290, Дубна, 1982.

Рукопись поступила в издательский отдел
10 мая 1988 года.