

**МОБИЛЬНАЯ
РЕЛЯЦИОННАЯ
СУБД**

ЛИНТЕР®

Linter Standard
Linter Bastion
Linter RealTime
Linter Multiversion

**Тестирование средств
защиты данных**

НАУЧНО-ПРОИЗВОДСТВЕННОЕ ПРЕДПРИЯТИЕ

 **РЕЛАКС®**

Товарные знаки

РЕЛЭКС™, ЛИНТЕР® , НЕВОД® , LAV™, ЛАКУНА являются товарными знаками, принадлежащими ЗАО НПП «Реляционные экспертные системы» (далее по тексту – компания РЕЛЭКС). Прочие названия и обозначения продуктов являются товарными знаками их производителей, продавцов или разработчиков.

Интеллектуальная собственность

Правообладателем продуктов ЛИНТЕР®, НЕВОД®, LAV™, ЛАКУНА является компания РЕЛЭКС (1990–2011). Все права защищены. Данный документ является собственностью компании РЕЛЭКС. Ни одна часть данного документа не может быть воспроизведена, передана, преобразована, сохранена в системе поиска информации, переведена на другой язык или компьютерный язык в какой-либо форме, какими-либо средствами, электронными, механическими, магнитными, оптическими, химическими, ручными или иными без предварительного разрешения компании РЕЛЭКС.

О документе

Материал, содержащийся в данном документе, прошел тщательную проверку, но компания РЕЛЭКС не гарантирует, что документ не содержит ошибок и пропусков. Компания РЕЛЭКС оставляет за собой право в любое время вносить в документ исправления и изменения, пересматривать и обновлять содержащуюся в нем информацию.

Адрес

394006, г. Воронеж, ул. 20-летия Октября, 119.
Тел./факс: (473) 2-711-711, 2-778-333.
e-mail: market@relex.ru.

Адрес для корреспонденции

394000, г. Воронеж, а/я 137.

Техническая поддержка

Отдел поддержки и сопровождения программных продуктов:

телефон: (473) 2-711-711 с 9:00 до 18:00 мск.
e-mail: support@relex.ru, market@relex.ru.

С целью повышения качества разрабатываемых программных средств и предоставляемых услуг в компании РЕЛЭКС действует автоматизированная система учёта и обработки рекламаций. Обо всех обнаруженных недостатках и ошибках в программном продукте и/или документации на него просим сообщать нам на Internet–странице [рекламация](#).

Оглавление

Предисловие	1
Назначение документа	1
Для кого предназначен документ	1
Принятые обозначения и соглашения	1
Дополнительные документы	3
Проверка средств защиты данных	4
Последовательность выполнения тестов	4
Тест реализации дискреционных правил разграничения доступа	4
Тест реализации мандатных правил разграничения доступа	4
Тест возможности маркировки документов	5
Тест контроля ввода/вывода на физическое устройство	5
Тест изоляции параллельно исполняемых запросов	5
Тест сопоставления пользователя с устройством	6
Тест регистрации событий	7
Тест контроля целостности КСЗ СУБД	7
Тест очистки памяти	7
Контроль дистрибуции	8
Описание тестов	9
Тест реализации дискреционных ПРД	9
Тест реализации мандатных ПРД	9
Тест очистки внешней памяти	10
Тест возможности маркировки документов	11
Тест контроля целостности КСЗ	11
Тест контроля ввода/вывода	12
Тест сопоставления пользователя с устройством	13
Тест регистрации событий	15
Тест изоляции параллельно выполняемых запросов	16
Тест контроля дистрибуции	17
Проверка требований ко 2 классу защиты информации	18
Запрет на доступ несанкционированного пользователя	18
Очистка оперативной и внешней памяти	18
Невозможность присвоения субъектом себе новых прав	18
Тестирование способов, связанных с дискреционным принципом контроля доступа (тест discret)	19
Реализация ПРД	21
Тестирование пользователя категории DBA	31
Идентификация и аутентификация	38
Контроль целостности КСЗ	38
Маркировка документов	38
Механизм надежного восстановления	39
Регистрация событий	39
Сопоставление пользователя с устройством и защита физических устройств	41
Контроль дистрибуции программных средств	46

Предисловие

Назначение документа

Документ предназначен для описания системы тестов, испытаний и результатов тестирования комплекса средств защиты информации (КСЗ) от несанкционированного доступа СУБД ЛИНТЕР.

Документ может использоваться для работы с любой версией СУБД ЛИНТЕР. Особенности конкретных версий оговариваются по тексту.

Для кого предназначен документ

Документ предназначен для администратора безопасности системы.

Набор тестов может использоваться для тестирования:



- реализации правил разграничения доступа (ПРД) (перехват явных и скрытых запросов, правильное распознавание санкционированных и несанкционированных запросов в соответствии с дискретными и мандатными правилами, средства защиты механизма разграничения доступа, санкционированные изменения ПРД);
- идентификации и аутентификации, а также их средств защиты;
- регистрации событий;
- средств защиты регистрационной информации и возможность санкционированного ознакомления с ней;
- работы механизма, осуществляющего контроль целостности СВТ;
- невозможности присвоения субъектом себе новых прав;
- очистки оперативной и внешней памяти и записи маскирующей информации в освобождаемые участки памяти;
- работы механизма изоляции процессов в оперативной памяти;
- маркировки документов;
- защиты ввода и вывода информации на отчуждаемый физический носитель и сопоставление пользователя с устройством;
- запрета на доступ несанкционированного пользователя;
- работы механизма надежного восстановления;
- средств контроля дистрибуции.

Принятые обозначения и соглашения

<u>Обозначение</u>	<u>Пример</u>	<u>Значение</u>
Курсив	<i>Растровым</i> называется изображение...	Новый термин в тексте
Полужирный шрифт	В этом случае необходимо переносить все физические файлы.	Выделение в тексте
Подчеркнутый шрифт	Подробную информацию о работе программы можно получить на сайте www.dmk.ru .	Адреса страниц Internet

Предисловие

<u>Обозначение</u>	<u>Пример</u>	<u>Значение</u>
Текст, разделенный знаком ⇒	Выполните команду View ⇒ Properties (Вид ⇒ Свойства).	Последовательность выполнения команд
Текст, заключенный в <>, со знаком + между ними	<Ctrl>+<C>	В <> заключаются клавиши клавиатуры, знак + означает сочетание клавиш
Крупный моноширинный текст	SQL> _q	Текст командной строки
Мелкий моноширинный текст	Page Time Count	Текст программы
Заглавные буквы	BROWSE	Названия команд, слова, зарезервированные в SQL, ключевые слова
Курсив в <>	<return statement>	Определяемый элемент синтаксической конструкции
Символ ::=		Равенство по определению. Слева от знака стоит определяемое понятие, справа – собственно определение понятия
Квадратные скобки []	DBSTORE [-d -n -o -p -r -t -u]	Необязательные элементы конструкции. В данном примере ключи не являются обязательными элементами команды
Вертикальная черта	<return value> ::= <value expression> NULL	Указывает на то, что все предшествующие ей элементы списка являются необязательными и могут быть заменены любым другим элементом списка после этой черты
Фигурные скобки { }	CODEPAGE {866 1251 KOI8}	Указывают на то, что все находящееся внутри них является единым целым
Многоточие «...»	Характеристики столбца MAKE CHAR(20) MODEL CHAR(20) ... SQL>	Означает, что предшествующая часть может быть повторена любое количество раз

Обозначение	Пример	Значение
Многоточие, внутри которого находится запятая «.,..»		Указывает, что предшествующая часть оператора, состоящая из нескольких элементов, разделенных запятыми, может иметь произвольное число повторений
Текст со знаком  на сером фоне	<div style="background-color: #e0e0e0; padding: 5px;">  Если конфигурация страницы-шаблона не учитывала свойств, команда будет выполнена некорректно. </div>	Примечание

Дополнительные документы

- СУБД ЛИНТЕР. Администрирование средств защиты данных.
- СУБД ЛИНТЕР. Системные таблицы.
- СУБД ЛИНТЕР. Модель защиты данных.

Проверка средств защиты данных

Перед началом тестирования комплекса средств защиты (КСЗ) необходимо выполнить подготовительные работы:

- 1) перенести тесты КСЗ СУБД ЛИНТЕР с CD-ROM «СУБД ЛИНТЕР. Тестовые программы» в рабочий каталог.
- 2) установить в переменной PATH путь на каталог исполняемых файлов СУБД ЛИНТЕР.
- 3) создать и настроить базу данных (БД) для тестирования:
 - при помощи утилиты gendb создать БД;
 - запустить локальное ядро СУБД ЛИНТЕР;
 - при помощи утилиты inl выполнить файл security.sql;
 - при помощи утилиты inl выполнить запрос:

```
grant access on unlisted station to all;
```

- остановить ядро СУБД ЛИНТЕР при помощи команды:

```
shut -u SYSTEM/MANAGER;
```

- вновь запустить ядро на этой же БД.

Последовательность выполнения тестов

 Примеры командных строк даны для ОС типа Unix.

Тест реализации дискреционных правил разграничения доступа

Запуск теста

```
./discret
```

Результаты

При успешном завершении теста будет выдано сообщение:

```
Test done. No errors found.  
The dropping of waste information.
```

Тест реализации мандатных правил разграничения доступа

Запуск теста

```
./mandat
```

Результаты

При успешном завершении теста будет выдано сообщение:

```
Test done. No errors found.Test has finished.
```

```
The Dropping of waste information.
Can't drop table dba1.d1t3! 2202
Can't drop table dba1.d1t4! 2202
```

 Последние 2 строки могут не выдаваться, так как они не связаны с процессом тестирования.

Тест возможности маркировки документов

Запуск теста

```
./marker
```

Результаты

При успешном завершении теста будет выдано сообщение:

```
Maximum group level (G) : 1
Maximum read level (R) : 6
Maximum write level (W) : 6
```

Тест контроля ввода/вывода на физическое устройство

Запуск

```
./device -create
```

Результаты

При успешном завершении должен быть создан файл device.log, в котором не должно быть строк, начинающихся с «Error».

Тест изоляции параллельно исполняемых запросов

Тестирование заключается в последовательном запуске shell-файлов из командной строки.

1. Создать набор файлов: 1.cmd, 2.cmd, 3.cmd командами:

```
echo -e "parall -table AA -logfile log1" >1.cmd
echo -e "parall -table BB -logfile log2" >2.cmd
echo -e "parall -table AA -logfile log3& \n parall -table BB -
logfile log4&" >3.cmd
```

2. Выполнить команду ОС:

```
chmod 777 *.cmd
```

3. При помощи утилиты inl создать пользователя USR1/USR1:

```
create user USR1 identified by 'USR1';
grant resource to USR1;
```

4. Запустить последовательно shell-файлы:

```
./1.cmd
./2.cmd
./3.cmd
```

5. При помощи стандартной программы сравнения файлов diff сравнить пары файлов в формате .log: log 1 и log3, log2 и log4:


```
diff log1 log3
diff log2 log4
```

Результаты

При сравнении в обоих случаях программа diff не должна найти никаких различий.

Тест сопоставления пользователя с устройством

Тест состоит из серверной и клиентской частей. Серверную часть stations запускают на той рабочей станции, где установлен сервер ЛИНТЕР, клиентскую часть userconn запускают на той рабочей станции, где установлен сетевой клиент ЛИНТЕР (условно назовем ее CLIENT01).

 В данной методике серверная и клиентская части располагаются на одной ЭВМ. Разница между сервером и клиентом заключается в том, что они работают в разных сессиях операционной системы.

Последовательность тестирования

1. На сервере следует запустить сетевой драйвер сервера, на клиенте CLIENT01 следует запустить сетевой драйвер клиента.
2. На сервере запускают серверную компоненту теста:
`./stations -create -station CLIENT01 -protocol tcpip -address 127.0.0.1`
3. После приглашения серверной компоненты теста:
`start userconn.exe -local on station CLIENT01, after that press any key to start next test`
на клиенте запускают сначала:
`./userconn -local`
4. Нажать клавишу <Enter> на серверной и на клиентской части.
5. Запустить на выполнение части компонент теста test4:
на клиенте запускают:
`./userconn`
6. Дальнейшие действия следует производить в соответствии с сообщениями, выводимыми программ, запущенных на сервере и на клиенте:
part1 на сервере, part1 на клиенте;
part2 на сервере, part2 на клиенте;
part3 на сервере, part3 на клиенте.
7. После приглашения серверной компоненты теста:
`start userconn.exe' test 4, after that press any key to start next test`
необходимо на сервере нажать клавишу <Enter> и будут запущены последующие тесты.
8. Нажать клавишу <Enter> на клиенте.
test5 на сервере, test5 на клиенте;
test6 на сервере, test6 на клиенте;
test7 на сервере, test7 на клиенте;
test8 на сервере, test8 на клиенте;
test9 на сервере, test9 на клиенте;
test10 на сервере, test10 на клиенте;
test11 на сервере, test11 на клиенте.

Результаты

При успешном завершении будут созданы файлы `local.log`, `remote.log` и `stations.log`. Эти файлы не должны содержать строк, начинающихся с «Error».

Тест регистрации событий

Перед запуском теста необходимо заново произвести подготовку БД.

Последовательность тестирования

1. Выполнить команду:
`./audtest1 -auditstart`
2. Перезапустить ядро ЛИНТЕР на той же БД, т.е. сначала подать команду `shut`, и снова запустить ядро ЛИНТЕР.
3. Запустить основную часть тестов:
`./audtest1 -check`
`./audtest2`

Результаты

В случае успешного завершения, тесты выдадут сообщение:

```
Test has started .....  
Test done. No errors found
```

Тест контроля целостности КСЗ СУБД

Последовательность тестирования

1. Подсчитать контрольную сумму к файлу `linter`, когда ядро работает:
`./count linter`
2. Смоделировать ситуацию некорректного завершения работы ядра ЛИНТЕР (например, сбой по выключению питания или удаление задачи `linter` при помощи команды `kill -9`);
3. После рестарта ОС повторно подсчитать контрольную сумму к файлу `linter`:
`./count linter`

Результаты

Контрольные суммы не должны совпадать.

Тест очистки памяти

Последовательность тестирования

1. Создать БД на гибком диске:
`mount /dev/fd0 /mnt/floppy`
`SY00=/mnt/floppy`
`gendb memdb.gdb`

2. Запустить локальное ядро на этой БД:

```
linter &
```

3. Создать системную таблицу аудита

```
inl -u SYSTEM/MANAGER
SQL>create table $$$audit (EventType SMALLINT, /* Event group */
                          EventId SMALLINT, /* Event type */
                          UserName CHAR(18), /* User name */
                          SourceAdr CHAR(24), /* Network address */
                          ObjectName CHAR(38),
                          ObjectType SMALLINT,
                          Body BYTE(58),
                          UserText CHAR(240)) maxrow 2;
```

4. Завершить работу СУБД ЛИНТЕР:

```
shut -u SYSTEM/MANAGER
```

5. Запустить повторно ядро СУБД:

```
linter &
```

6. Запустить тест:

```
./memtest1
```

7. Завершить работу СУБД ЛИНТЕР:

```
shut -u SYSTEM/MANAGER
```

8. Запустить тест:

```
./memtest2
```

При этом должно быть найдено 2 записи.

9. Запустить ядро СУБД

```
linter &
```

10. Запустить тест:

```
./memtest1 /drop
```

11. Завершить работу СУБД ЛИНТЕР:

```
shut -u SYSTEM/MANAGER
```

12. Повторить пункт 8, при этом должна быть найдена 1 запись.

Контроль дистрибуции

Запуск

```
./count linter.tar.Z
```

где `linter.tar.Z` – это дистрибутивный комплект ЛИНТЕР.

Результаты

Производится подсчет контрольной суммы. Результаты должны совпадать с эталонными.

Описание тестов

Этот раздел содержит описание тестов, используемых для подтверждения правильного функционирования КСЗ СУБД ЛИНТЕР.

Тест реализации дискреционных ПРД

Назначение теста

Тест `discret` предназначен для тестирования реализации дискреционных ПРД. Он осуществляет проверку успешности осуществления идентификации и аутентификации, правильности распознавания санкционированных и несанкционированных запросов на доступ, механизма разграничения доступа, а также возможность санкционированного изменения ПРД.

Исходный текст теста находится в документе «СУБД ЛИНТЕР Тестовые программы».

Описание теста

В процессе работы теста в БД создаются:

1) пользователи:

Имя	Пароль	Категория
CONN1	CONNP1	Connect
CONN2	CONNP2	Connect
RES1	RESP1	Resource
RES2	RESP2	Resource
DBA1	DBAP1	Db

2) роли:

- роль `com_user1` - назначена пользователям `CONN1`, `RES1`;
- роль `com_user2` - назначена пользователям `CONN2`, `RES2`.

У пользователя `RES1` есть таблицы `r1t1`, `r1t2`. На таблицу `r1t1` создан общедоступный (`PUBLIC`) синоним `res1tab1`. Столбец `PersID` таблицы `r1t2` проиндексирован.

У пользователя `RES2` есть таблицы `r2t1`, `r2t2`. На таблицу `r2t2` создан общедоступный (`PUBLIC`) синоним `res2tab2` и создано представление `allt2`. Столбец `PersID` таблицы `r2t2` проиндексирован.

Если указанных объектов к моменту запуска теста не было в БД, то `discret` их создаст.

Запуск теста

Запуск задачи производится командной строкой:

```
discret
```

Тест реализации мандатных ПРД

Назначение теста

Тест `mandat` предназначен для проверки мандатных ПРД СУБД ЛИНТЕР. Мандатная защита обеспечивается разбиением пользователей на группы и присвоения им, а также

данным, меток уровней доступа. Полную информацию об этом можно получить в технической документации.

Исходный текст теста находится в документе «СУБД ЛИНТЕР Тестовые программы».

Описание теста

Перед началом тестов в БД создаются:

- 1) группы: GROUP1, GROUP2 - флаги доверия между ними не установлены.
- 2) уровни: four = 4, five = 5, six = 6.
- 3) пользователи:
DBA1(R =W =5), RES1(R =W =5) - в группе GROUP1;
DBA2(R =W =5), RES2 (R =6, W =4) - в группе GROUP2.
- 4) у пользователя RES2 есть таблицы:
 - R2T1(R =5, W =5) из 10 строк. Уровень доступа для 4 строк со значением атрибута PersID=2: R5W5, R6W6, R6W5, R5W6; для 4 строк со значением атрибута PersID=1 уровни доступа к полю MODEL1: R5W5, R6W6, R6W5, R5W6; для 2 строк с PersID=10,11 уровни доступа: R5W5;
 - R2T2(R =5, W =6);
 - R2T3(R =6, W =5);
 - R2T4(R =6, W =6) из 8 строк. Уровень доступа для 4 строк со значением атрибута PersID=2: R5W5, R6W6, R6W5, R5W6; для 4 строк со значением атрибута PersID=1 уровни доступа к полю MODEL4: R5W5, R6W6, R6W5, R5W6; для 2 строк с PersID=10,11 уровни доступа: R5W5;
 - R2T5(R =5, W =5) - есть атрибут MODEL5(R =6, W =6);
 - R2T6(R =5, W =5) - есть атрибут MODEL6(R =5, W =6);
 - R2T7(R =5, W =5) - есть атрибут MODEL7(R =6, W =5);
 - R2T8(R =5, W =5).

Таблицы R2T2, R2T3, R2T5, R2T6, R2T7, R2T8 содержат по 3 строки.
DBA1 и RES1 имеют привилегию ALL на все таблицы.

Запуск теста

mandat

Тест очистки внешней памяти

Назначение теста

Тесты memtest1, memtest2 предназначены для проверки перераспределения внешней памяти при удалении таблиц.

Тест memtest1 предназначен для создания и удаления таблиц, memtest2 - для подсчета числа появления тестовой строки на дискете.

Исходный текст теста находится в документе «СУБД ЛИНТЕР Тестовые программы».

Описание теста

Тестируемая БД должна располагаться на гибком диске. Очередь файлов должна быть равной четырем. Для этого необходимо запустить утилиту `gendb` и подать команду `SET FILES 4;`.

Запуск тестов

```
memtest1 [/drop]
memtest2
```

Ключ `/drop` заставляет удалять таблицы.

Тест возможности маркировки документов

Назначение теста

Тест `marker` предназначен для проверки возможности получения данных БД и их меток доступа посредством SQL-запросов с функцией `SECURITY`.

Исходный текст теста находится в документе «СУБД ЛИНТЕР Тестовые программы».

Описание теста

Тестируемая БД должна содержать все таблицы для осуществления контроля доступа (`LEVEL`, `GROUP` и пр.).

Запуск теста

```
marker
```

Тест контроля целостности КСЗ

Назначение теста

Тест предназначен для контроля целостности комплекса средств защиты СУБД ЛИНТЕР путем подсчета 32-битной контрольной суммы файла.

Производится расчет 16-байтной последовательности символов, однозначно идентифицирующих заданный файл. Расчет производится с использованием распространенного алгоритма вычисления аутентифицирующих кодов `Message Digest` в режиме сцепления по промежуточному результату вычислений.

Затем результат суммируется со сдвигом для получения результирующей 32-битной контрольной суммы.

Тестирование механизма контроля целостности заключается в следующем. Производится подсчет контрольной суммы каждого файла каталога. Затем этот каталог копируется в отдельный тестовый каталог, и с помощью любого редактора файлов производятся минимальные изменения содержимого некоторого файла. Задача `count` повторно прогоняется через тестовый каталог. Тест считается успешным, если результаты программы `count` в первом случае отличаются от результатов во втором случае.

Запуска теста

```
count <имя_файла>
```

Тест контроля ввода/вывода

Назначение теста

Тест device предназначен для тестирования реализации физических устройств в структуре КСЗ СУБД ЛИНТЕР.

Исходный текст теста находится в документе «СУБД ЛИНТЕР Тестовые программы».

Описание теста

Тестирование работает на «чистой БД» или на БД со следующими настройками:

- 1) уровни доступа:

\$\$\$ID	\$\$\$NAME
1	LEV1
2	LEV2
3	LEV3
4	LEV4
5	LEV5
6	LEV6
7	LEV7
8	LEV8
9	LEV9
10	LEV10

- 2) группы:

\$\$\$ID	\$\$\$NAME
1	GR1
2	GR2
3	GR3
4	GR4
5	GR5
6	GR6
7	GR7
8	GR8
9	GR9
10	GR10

В том случае, если в БД уже были уровни или группы с указанными ID, но с другими именами, то их имена будут изменены на указанные выше.

Запуск теста

device [ключ [ключ ...]]

Ключи теста

<u>Ключ</u>	<u>Описание</u>
/HELP	«Подсказка»
/CREATE 1	Создание перед запуском теста уровней и групп. Необходимо использовать при первом запуске теста
/ADM	ID администратора безопасности системы; по умолчанию – SYSTEM
/PASSWD	Пароль администратора безопасности системы, по умолчанию – MANAGER
/IS	Уровень изоляции доступа, в котором работает тест (точнее, соединение с ЛИНТЕР администратора безопасности); по умолчанию – autocommit

Ключ	Описание
/USER	ID пользователя; по умолчанию – USER1. Имя SYSTEM (или ID администратора безопасности) не допускается, в этом случае ID и пароль будут заменены значениями по умолчанию, то есть USER1/USER1
/PASSWORD	Пароль пользователя; по умолчанию – USER1
/DEVICE	Имя физического устройства; по умолчанию - DV01, SY00 не допускается, в этом случае значение будет изменено на значение по умолчанию, то есть на DV01
/PATH	Путь устройства, по умолчанию - путь устройства SY00, а если в таблице \$\$\$DEVICE не будет найдено устройство с таким именем, то поиск выполняется в текущем каталоге
/TABLE	Имя таблицы, по умолчанию – ZZ; если в БД была таблица с указанным именем, то она будет уничтожена и создана тестовая таблица
/ROWS	Число записей в таблице, по умолчанию – 100
/CONT	Длительность циклов теста, по умолчанию – 1

Пример запуска теста

```
device /adm SYSTEM /password ZZZ /user AAA /password BBV
/table qw /device dev1 /path /VAR/TMP /rows 1000
```

Тест сопоставления пользователя с устройством

Назначение теста

Тесты stations и userconn предназначены для тестирования реализации сетевых устройств в структуре КСЗ СУБД ЛИНТЕР.

Исходный текст теста находится в документе «СУБД ЛИНТЕР Тестовые программы».

Описание теста

Тесты работают на «чистой БД» или на БД со следующими настройками:

- 1) уровни:

\$\$\$ID	\$\$\$NAME
1	LEV1
2	LEV2
3	LEV3
4	LEV4
5	LEV5
6	LEV6
7	LEV7
8	LEV8
9	LEV9
10	LEV10

- 2) группы:

\$\$\$ID	\$\$\$NAME
1	GR1
2	GR2
3	GR3
4	GR4
5	GR5
6	GR6

7	GR7
8	GR8
9	GR9
10	GR10

В том случае, если в БД были уровни или группы с указанными ID, то их имена будут изменены на указанные выше.


Перед началом теста администратор с локальной машины должен выполнить следующие действия:

```
in1 -u SYSTEM/MANAGER
SQL> GRANT ACCESS ON UNLISTED STATION TO ALL;
SQL> EXIT
```

Запуск теста stations

```
stations [ключ [ключ ...]]
```

Ключи теста

<u>Ключ</u>	<u>Описание</u>
/HELP	Напечатать «Подсказку»
/CREATE 1	Создание перед запуском теста уровней и групп. Необходимо использовать при первом запуске теста
/NODE	Имя ЛИНТЕР-сервера; по умолчанию RELEX
/ADM	ID администратора безопасности системы; по умолчанию – SYSTEM
/PASSWD	Пароль администратора безопасности системы, по умолчанию – MANAGER
/IS	Уровень изоляции доступа, в котором работает тест (точнее, соединение с ЛИНТЕР администратора безопасности); по умолчанию – <code>autocommit</code>
/USER	ID пользователя; по умолчанию – USER1. Имя SYSTEM (или ID администратора безопасности) не допускается, в этом случае ID и пароль будут заменены значениями по умолчанию, то есть USER1/USER1
/PASSWORD	Пароль пользователя; по умолчанию – USER1
/STATION	Имя станции
/ADDRESS	Адрес станции
/PROTOCOL	Сетевой протокол; допустимые значения: TCPIP;  Согласованность параметров /STATION, /ADDRESS, /PROTOCOL программно не отслеживается, это необходимые параметры
/TABLE	Имя таблицы, по умолчанию – ZZ; если в БД была таблица с указанным именем, то она будет уничтожена и создана тестовая таблица
/ROWS	Число записей в таблице, по умолчанию – 100
/CONT	Длительность циклов теста, по умолчанию – 1

Тест stations может запускаться как с локальной машины, так и с удаленной.

Пример запуска

```
stations /adm SYSTEM /password ZZZ /user AAA /password BBB
/station server01 /address 190.222.33.111 /table as /rows 1000
```

Тест userconn используется в паре с тестом stations на рабочей станции с именем COMPUTERNAME для тестирования соединения с ЛИНТЕР-сервером.

Запуск теста userconn

```
stations [ключ [ключ ...]]
```

Ключи теста

Ключ	Описание
/HELP	Напечатать «Подсказку»
/IS	Уровень изоляции доступа, в котором работает тест (точнее, соединение с ЛИНТЕР администратора безопасности); по умолчанию – autocommit
/USER	ID пользователя; по умолчанию – USER1 . Имя SYSTEM (или ID администратора безопасности) не допускается, в этом случае ID и пароль будут заменены значениями по умолчанию, то есть USER1/USER1
/PASSWORD	Пароль пользователя; по умолчанию – USER1
/TABLE	Имя таблицы, по умолчанию – ZZ ; если в БД была таблица с указанным именем, то она будет уничтожена и создана тестовая таблица
/ROWS	Число записей в таблице, по умолчанию – 100
/CONT	Длительность циклов теста, по умолчанию – 1
/LOCAL	Запуск теста без повторений, об успешном прохождении теста свидетельствует сообщение test passed

Работа userconn происходит в режиме согласования с stations, о старте теста свидетельствует приглашение:

```
start test <номер теста>, press any key to start
```

Тест регистрации событий

Назначение теста

Тесты audtest1, audtest2 предназначены для проверки возможности регистрации событий, связанных с КСЗ СУБД ЛИНТЕР.

Тест audtest1 проверяет только регистрацию *загрузки ядра СУБД ЛИНТЕР и завершения его работы*.

Тест audtest2 проверяет регистрацию большой группы событий.

Исходный текст теста находится в документе «СУБД ЛИНТЕР Тестовые программы».

Запуск теста audtest1

```
audtest1 [ключ [ключ ...]]
```

Ключи теста

<u>Ключ</u>	<u>Описание</u>
AUDITSTART	Запуск системы регистрации событий и разрешение регистрации событий старта и завершения работы СУБД ЛИНТЕР
CHECK	Проверка регистрации событий, разрешенных тестом audtest1 – auditstart

Запуск теста audtest2 audtest2

Тест изоляции параллельно выполняемых запросов

Назначение теста

Тестирование изоляции модулей проводится с целью проверки надежности механизмов изоляции выполняющихся параллельно запросов в СУБД ЛИНТЕР.

Исходный текст теста находится в документе «СУБД ЛИНТЕР. Тестовые программы».

Описание теста

Тестирование состоит из двух этапов.

Первый этап - запуск последовательно двух задач, работающих с непересекающимися данными из БД и фиксирование соответственно двух групп результатов.

Второй этап представляет собой запуск тех же задач, но параллельно и фиксирование второй пары результатов. Тест считается успешным, если результаты работы каждой задачи в обоих случаях совпадают.

Тест parall создает таблицу (если указан ключ /CREATE), добавляет записи и выполняет 3 различные выборки из таблицы. Требуется запуск теста двумя разными пользователями (например, USER1 и USER2). В случае указания ключа /CREATE необходима привилегия RESOURCE, или запуск тестов одним пользователем, но над разными таблицами (например, TABLE1 и TABLE2). Во всех остальных случаях тесты работают с пересекающимися данными.

Запуск теста

parall [ключ [ключ ...]]

Ключи теста

<u>Ключ</u>	<u>Описание</u>
/HELP	Напечатать «Подсказку»
/LOG	Имя лог-файла; необходимо, чтобы имена лог-файлов были разные для параллельно запускаемых утилит
/TABLE	Имя таблицы, по умолчанию – ZZ; если в БД была таблица с указанным именем, то она будет уничтожена и создана тестовая таблица
/COLUMNS	Количество колонок типа int и типа byte (максимальное значение - 49, по умолчанию - 49)

Ключ	Описание
/TABLE	Имя таблицы, по умолчанию – ZZ; если в БД была таблица с указанным именем, то она будет уничтожена и создана тестовая таблица
/USER	ID пользователя; по умолчанию – USER1. Имя SYSTEM (или ID администратора безопасности) не допускается, в этом случае ID и пароль будут заменены значениями по умолчанию, то есть USER1/USER1
/PASSWORD	Пароль пользователя; по умолчанию – USER1
/CREATE 1	Создание перед запуском теста уровней и групп. Необходимо использовать при первом запуске теста
/IS	Уровень изоляции доступа, в котором работает тест (точнее, соединение с ЛИНТЕР администратора безопасности); по умолчанию – autocommit
/ROWS	Число записей в таблице, по умолчанию – 100
/CONT	Длительность циклов теста, по умолчанию – 1

Запуск теста

Сначала следует запустить тест последовательно, например:

```
parall /log log1 /user urs1 /password usr1
parall /log log2 /user urs2 /password usr2
```

Затем эти 2 теста запускаются параллельно, например bath-файл, содержащий строки:

```
parall /log log3 /user urs1 /password usr1
parall /log log4 /user urs2 /password usr2
```

Далее следует сравнить файлы log1 и log3, log2 и log4. Тест считается успешным, если попарно совпадают log1 и log3, log2 и log4.

Тест контроля дистрибуции

Назначение теста

Тест контроля дистрибуции СУБД ЛИНТЕР предназначена для проверки точности копирования при изготовлении копий дистрибутивного комплекта с эталонного образца, проверки целостности хранящейся копии, а также для проверки копии на случайную или злонамеренную ее модификацию.

Описание теста

Контроль дистрибуции осуществляется путем подсчета и сравнения контрольных сумм всех дистрибутивных файлов (эталонной контрольной суммы дистрибутивного комплекта), с соответствующими контрольными суммами комплекта - копии.

Эталонная контрольная сумма приводится в документации, поставляемой вместе с дистрибутивным комплектом СУБД ЛИНТЕР.

Система контроля дистрибуции применяется как разработчиками - при изготовлении копий дистрибутива, так и пользователями - перед процессом инсталляции. Рекомендуется осуществлять проверку соответствия копии эталону перед каждой процедурой инсталляции.

Запуск теста

count <имя_файла>

Проверка требований ко 2 классу защиты информации

В данном разделе подробно описано, каким образом выполняется проверка тестами требований, предъявляемых ко 2 классу защиты информации.

Запрет на доступ несанкционированного пользователя

Проверяется тестом discret.

Тест проверяет попытку открытия каналов несуществующими в БД пользователями или существующими, но использующими неверные пароли.

Реализация

<u>Пользователь</u>	<u>Действие</u>
NEW	Попытка открытия канала. Результат: код завершения 1025
CONN1	Попытка открытия канала с неверным паролем. Результат: код завершения 1026
RES1	Попытка открытия канала с неверным паролем. Результат: код завершения 1026
DVA1	Попытка открытия канала с неверным паролем. Результат: код завершения 1026

Очистка оперативной и внешней памяти

Проверяется тестом memtest.

Перераспределение внешней памяти, занимаемой файлами базы данных, может происходить только в двух случаях: расширении таблиц и удалении таблиц. При изменении содержимого таблиц (удалении данных) перераспределения не происходит. Для тестирования освобождения внешней памяти анализируется содержимое памяти до, и после удаления некоторой таблицы.

Реализация

- 1) на гибком диске создается БД. Очередь файлов БД устанавливается равной 4 файлам;
- 2) в процессе работы теста создаются таблицы TEST1, TEST2, TEST3, TEST4, состоящие из 1 столбца типа char(20). В таблицу TEST1 заносится строка TESTING. С помощью последующего открытия таблиц TEST2, TEST3, TEST4 таблица TEST1 вытесняется на диск;
- 3) производится сканирование диска для определения количества строк TESTING;
- 4) производится удаление таблицы TEST1;
- 5) повторяется сканирование диска. Если количество строк TESTING не изменилось, значит, очистки памяти не происходит, иначе остаточная информация удаляется.

Невозможность присвоения субъектом себе новых прав

Проверяется тестами discret, mandat.

Присвоение субъектом себе новых прав может произойти несколькими способами: изменения субъектом своей категории, назначения себе привилегий на чужие таблицы, изменения им своей группы, изменения им своих уровней доступа.

Тестирование способов, связанных с дискреционным принципом контроля доступа (тест *discret*)

Реализация

<u>Таблица</u>	<u>Пользователь</u>	<u>Действие</u>
	CONN1	Попытка предоставления себе привилегии Resource . Результат: код завершения 1022
res1.r1t1	CONN1	Попытка предоставления себе прав доступа select на таблицу. Результат: код завершения 1022
res1.r1t1	CONN1	Попытка предоставления себе прав доступа insert на таблицу. Результат: код завершения 1022
res1.r1t1	CONN1	Попытка предоставления себе прав доступа delete на таблицу. Результат: код завершения 1022
res1.r1t1	CONN1	Попытка предоставления себе прав доступа update на таблицу. Результат: код завершения 1022
res1.r1t1	CONN1	Попытка предоставления себе прав доступа index на таблицу. Результат: код завершения 1022
res1.r1t1	CONN1	Попытка предоставления себе прав доступа alter на таблицу. Результат: код завершения 1022
res1.r1t1	CONN1	Попытка предоставления себе прав доступа all на таблицу. Результат: код завершения 1022
	RES1	Попытка предоставления себе привилегии Db . Результат: код завершения 1022
res2.r2t1	RES1	Попытка предоставления себе прав доступа select на таблицу. Результат: код завершения 1022
res2.r2t1	RES1	Попытка предоставления себе прав доступа insert на таблицу. Результат: код завершения 1022
res2.r2t1	RES1	Попытка предоставления себе прав доступа delete на таблицу. Результат: код завершения 1022
res2.r2t1	RES1	Попытка предоставления себе прав доступа update на таблицу. Результат: код завершения 1022

<u>Таблица</u>	<u>Пользователь</u>	<u>Действие</u>
res2.r2t1	RES1	Попытка предоставления себе прав доступа <code>index</code> на таблицу. Результат: код завершения 1022
res2.r2t1	RES1	Попытка предоставления себе прав доступа <code>alter</code> на таблицу. Результат: код завершения 1022
res2.r2t1	RES1	Попытка предоставления себе прав доступа <code>all</code> на таблицу. Результат: код завершения 1022
res1.r1t1	DBA1	Попытка предоставления себе прав доступа <code>select</code> на таблицу. Результат: код завершения 1022
res1.r1t1	DBA1	Попытка предоставления себе прав доступа <code>insert</code> на таблицу. Результат: код завершения 1022
res1.r1t1	DBA1	Попытка предоставления себе прав доступа <code>delete</code> на таблицу. Результат: код завершения 1022
res1.r1t1	DBA1	Попытка предоставления себе прав доступа <code>update</code> на таблицу. Результат: код завершения 1022
res1.r1t1	DBA1	Попытка предоставления себе прав доступа <code>index</code> на таблицу. Результат: код завершения 1022
res1.r1t1	DBA1	Попытка предоставления себе прав доступа <code>alter</code> на таблицу. Результат: код завершения 1022
res1.r1t1	DBA1	Попытка предоставления себе прав доступа <code>all</code> на таблицу. Результат: код завершения 1022

Тестирование способов, связанных с мандатным принципом контроля доступа (тест `mandat`)

Реализация

<u>Пользователь</u>	<u>Действие</u>
SYSTEM	Попытка изменения группы пользователя <code>RES1</code> . Результат: успешное завершение (<code>RES1</code> возвращает группу <code>GROUP1</code>)
SYSTEM	Попытка изменения своей группы. Результат: код завершения 1022
DBA1	Попытка изменения своей группы. Результат: код завершения 1022 (изменить уровни доступа пользователя может только администратор его группы (в пределах отведенных ему уровней) или <code>SYSTEM</code>)
DBA1	Попытка изменения своих уровней доступа <code>R=6</code> , <code>W=5</code> . Результат: код завершения 1022

<u>Пользователь</u>	<u>Действие</u>
DBA1	Попытка изменения своих уровней доступа R=5, W=4. Результат: код завершения 1022
DBA1	Попытка изменения своих уровней доступа R=4, W=6. Результат: успешное завершение
RES1	Попытка изменения своих уровней доступа R=6, W=5. Результат: код завершения 1022
RES1	Попытка изменения своих уровней доступа R=5, W=4. Результат: код завершения 1022
RES1	Попытка изменения своих уровней доступа R=4, W=6. Результат: код завершения 1022
RES1	Попытка изменения своей группы. Результат: код завершения 1022
SYSTEM	Попытка изменения своих уровней доступа R=6, W=6. Результат: успешное завершение
SYSTEM	Попытка изменения своих уровней доступа R=4, W=4. Результат: успешное завершение (уровни доступа пользователей RES1 и DBA1 устанавливаются R=5, W=5)

Реализация ПРД

Проверяется тестами discret, mandat.

Для проверки реализации ПРД в СУБД ЛИНТЕР проводятся две группы тестов, осуществляющие различные операции с субъектами и объектами БД.

К первой группе тестов относится **тестирование функционирования дискреционных ПРД**. Здесь производится проверка возможностей пользователей с различными уровнями привилегий: Connect, Resource, DbA.

Для каждой категории проверка производится в два этапа.

На первом этапе данный пользователь пытается совершать действия, запрещенные ему как представителю определенной категории и независимые от его прав на конкретные объекты.

На втором этапе тестируется возможность совершения им действий над чужими объектами, потенциально разрешенных ему предоставленной категорией, но с учетом различных прав на данный объект, предоставленных владельцем данного объекта.

Тестирование пользователя категории CONNECT

Для пользователя категории CONNECT на первом этапе тестируется его способность создавать новых пользователей, удалять уже существующих, предоставлять и отбирать различные уровни привилегий других пользователей, а также предоставление прав доступа пользователям на чужие таблицы. Производятся попытки уничтожения уже существующих и создания новых ролей, а также предоставление и отбор привилегий пользователей на эту роль.

Те же попытки производятся по отношению к представлению. Проверяется невозможность создания пользователем этой категории собственных таблиц.

На втором этапе (см. с. 23) проводятся попытки совершения действий, потенциально зависящих от прав доступа пользователя по отношению к конкретному объекту: попытки уничтожения таблиц других пользователей, создания и уничтожения индексов, изменения структуры таблиц. Тестируется возможность чтения, добавления, изменения содержимого таблиц с различными правами доступа к ним.

Реализация

<u>Таблица</u>	<u>Пользователь</u>	<u>Действие</u>
	CONN1	Попытка создания таблицы <code>clt1</code> . Результат: код завершения 1022
	CONN1	Попытка создания пользователя <code>Axe1/axe1p</code> категории <code>CONNECT</code> . Результат: код завершения 1022
	CONN1	Попытка создания пользователя <code>Axe1/axe1p</code> категории <code>RESOURCE</code> . Результат: код завершения 1022
	CONN1	Попытка создания пользователя <code>Axe1/axe1p</code> категории <code>DBA</code> . Результат: код завершения 1022
<code>res1.r1t1</code>	CONN1	Попытка предоставления прав доступа <code>select</code> пользователям <code>res2</code> . Результат: код завершения 1022
<code>res2.r2t1</code>	CONN1	Попытка предоставления прав доступа <code>select</code> пользователям <code>res2</code> . Результат: код завершения 2152
<code>res1.r1t1</code>	CONN1	Попытка предоставления прав доступа <code>select</code> пользователям <code>dba1</code> . Результат: код завершения 1022
<code>res2.r2t1</code>	CONN1	Попытка предоставления прав доступа <code>select</code> пользователям <code>dba1</code> . Результат: код завершения 1022
	CONN1	Попытка отмены привилегии <code>RESOURCE</code> у пользователя <code>res2</code> . Результат: код завершения 1022
<code>res1.r1t1</code>	CONN1	Попытка отмены права <code>select</code> у пользователя <code>res2</code> . Результат: код завершения 1022
<code>res2.r2t1</code>	CONN1	Попытка отмены права <code>select</code> у пользователя <code>res2</code> . Результат: код завершения 2152
	CONN1	Попытка удаления пользователя <code>res1</code> . Результат: код завершения 1022
	CONN1	Попытка удаления пользователя <code>conn1</code> . Результат: код завершения 1022
	CONN1	Попытка изменения пароля пользователя <code>res1</code> . Результат: код завершения 1022
	CONN1	Попытка удаления ролей <code>com_user1</code> . Результат: код завершения 1022

<u>Таблица</u>	<u>Пользователь</u>	<u>Действие</u>
	CONN1	Попытка удаления ролей <code>com_user2</code> . Результат: код завершения 1022
	CONN1	Попытка создания роли <code>com_user3</code> . Результат: код завершения 1022
res1.r1t1	CONN1	Попытка предоставления привилегий <code>insert</code> на таблицу для роли <code>com_user1</code> . Результат: код завершения 1022
res1.r1t1	CONN1	Попытка предоставления привилегий <code>select</code> на таблицу для роли <code>com_user1</code> . Результат: код завершения 1022
Роль: com_user1	CONN1	Попытка назначения роли пользователю <code>res2</code> . Результат: код завершения 1022
	CONN1	Попытка отобразить роль <code>com_user1</code> у пользователя <code>res1</code> . Результат: код завершения 1022
res1.r1t2	CONN1	Попытка создания представления на таблицу. Результат: код завершения 1022
	CONN1	Попытка уничтожения представления <code>res2.allt2</code> . Результат: код завершения 2133
res1.r1t2	CONN1 (без уровня прав <code>select</code>)	Попытка выполнить <code>select</code> -запрос. Результат: код завершения 1022
	CONN1 (без уровня прав <code>select</code>)	Попытка выполнить <code>select</code> -запрос через синоним <code>res1.tab1</code> . Результат: код завершения 1022
res1.r1t1	CONN1 (привилегия <code>select</code> на таблицу)	Попытка удаления таблицы. Результат: код завершения 2133
res1.r1t2	CONN1 (привилегия <code>select</code> на таблицу)	Попытка выполнить <code>insert</code> -запрос. Результат: код завершения 1022
res1.r1t2	CONN1 (привилегия <code>select</code> на таблицу)	Попытка выполнить <code>update</code> запрос. Результат: код завершения 1022
res1.r1t2	CONN1 (привилегия <code>select</code> на таблицу)	Попытка выполнить <code>delete</code> -запрос. Результат: код завершения 1022
res1.r1t2	CONN1 (привилегия <code>select</code> на таблицу)	Попытка создания индекса. Результат: код завершения 1022
res1.r1t2	CONN1 (привилегия <code>select</code> на таблицу)	Попытка удаления индекса. Результат: код завершения 1022
res1.r1t1	CONN1 (привилегия <code>select</code> на таблицу)	Попытка изменения структуры таблицы (добавление столбца). Результат: код завершения 1022

<u>Таблица</u>	<u>Пользователь</u>	<u>Действие</u>
res1.r1t1	CONN1 (привилегия select на таблицу)	Попытка создания синонима. Результат: код завершения 1022
res1.r1t1	CONN1 (привилегии select, insert на таблицу)	Попытка удаления таблицы. Результат: код завершения 2133
res1.r1t2	CONN1 (привилегии select, insert на таблицу)	Попытка выполнить update-запрос. Результат: код завершения 1022
res1.r1t2	CONN1 (привилегии select, insert на таблицу)	Попытка выполнить delete-запрос. Результат: код завершения 1022
res1.r1t2	CONN1 (привилегии select, insert на таблицу)	Попытка создания индекса. Результат: код завершения 1022
res1.r1t2	CONN1 (привилегии select, insert на таблицу)	Попытка удаления индекса. Результат: код завершения 1022
res1.r1t1	CONN1 (привилегии select, insert на таблицу)	Попытка изменения структуры таблицы (добавление столбца). Результат: код завершения 1022
res1.r1t1	CONN1 (привилегии select, insert на таблицу)	Попытка создания синонима. Результат: код завершения 1022
res1.r1t1	CONN1 (привилегии select, insert, update на таблицу)	Попытка удаления таблицы. Результат: код завершения 2133
res1.r1t2	CONN1 (привилегии select, insert, update на таблицу)	Попытка выполнить delete-запрос. Результат: код завершения 1022
res1.r1t2	CONN1 (привилегии select, insert, update на таблицу)	Попытка создания индекса. Результат: код завершения 1022
res1.r1t2	CONN1 (привилегии select, insert, update на таблицу)	Попытка удаления индекса. Результат: код завершения 1022
res1.r1t1	CONN1 (привилегии select, insert, update на таблицу)	Попытка изменения структуры таблицы (добавление столбца). Результат: код завершения 1022
res1.r1t1	CONN1 (привилегии select, insert, update на таблицу)	Попытка создания синонима. Результат: код завершения 1022

<u>Таблица</u>	<u>Пользователь</u>	<u>Действие</u>
res1.r1t1	CONN1 (привилегии select, insert, update, delete на таблицу)	Попытка удаления таблицы. Результат: код завершения 2133
res1.r1t2	CONN1 (привилегии select, insert, update, delete на таблицу)	Попытка создания индекса. Результат: код завершения 1022
res1.r1t2	CONN1 (привилегии select, insert, update, delete на таблицу)	Попытка удаления индекса. Результат: код завершения 1022
res1.r1t1	CONN1 (привилегии select, insert, update, delete на таблицу)	Попытка изменения структуры таблицы (добавление столбца). Результат: код завершения 1022
res1.r1t1	CONN1 (привилегии select, insert, update, delete на таблицу)	Попытка создания синонима. Результат: код завершения 1022
res1.r1t1	CONN1 (привилегии select, insert, update, delete, alter на таблицу)	Попытка удаления таблицы. Результат: код завершения 2133
res1.r1t2	CONN1 (привилегии select, insert, update, delete, alter на таблицу)	Попытка создания индекса. Результат: код завершения 1022
res1.r1t2	CONN1 (привилегии select, insert, update, delete, alter на таблицу)	Попытка удаления индекса. Результат: код завершения 1022
res1.r1t1	CONN1 (привилегии select, insert, update, delete, alter на таблицу)	Попытка изменения структуры таблицы (добавление столбца). Результат: код завершения 1022

<u>Таблица</u>	<u>Пользователь</u>	<u>Действие</u>
res1.r1t1	CONN1 (привилегии select, insert, update, delete, alter на таблицу)	Попытка создания синонима. Результат: код завершения 1022
res1.r1t1	CONN1 (привилегии select, insert, update, delete, alter, index на таблицу)	Попытка удаления таблицы. Результат: код завершения 2133
res1.r1t2	CONN1 (привилегии select, insert, update, delete, alter, index на таблицу)	Попытка создания индекса. Результат: код завершения 1022
res1.r1t2	CONN1 (привилегии select, insert, update, delete, alter, index на таблицу)	Попытка удаления индекса. Результат: код завершения 1022
res1.r1t1	CONN1 (привилегии select, insert, update, delete, alter, index на таблицу)	Попытка изменения структуры таблицы (добавление столбца). Результат: код завершения 1022
res1.r1t1	CONN1 (привилегии select, insert, update, delete, alter, index на таблицу)	Попытка создания синонима. Результат: код завершения 1022
res1.r1t1	CONN1 (привилегии select, insert, update, delete, alter, index, all на таблицу)	Попытка удаления таблицы. Результат: код завершения 2133
res1.r1t2	CONN1 (привилегии select, insert, update, delete, alter, index, all на таблицу)	Попытка создания индекса. Результат: код завершения 1022

<u>Таблица</u>	<u>Пользователь</u>	<u>Действие</u>
res1.r1t2	CONN1 (привилегии select, insert, update, delete, alter, index, all на таблицу)	Попытка удаления индекса. Результат: код завершения 1022
res1.r1t1	CONN1 (привилегии select, insert, update, delete, alter, index, all на таблицу)	Попытка изменения структуры таблицы (добавление столбца). Результат: код завершения 1022
res1.r1t1	CONN1 (привилегии select, insert, update, delete, alter, index, all на таблицу)	Попытка создания синонима. Результат: код завершения 1022
res1.r1t2	CONN1 (привилегия all на таблицу)	Попытка создания представления. Результат: код завершения 1022

Тестирование пользователя категории RESOURCE

Для пользователя категории RESOURCE на первом этапе тестируется его способность создавать новых пользователей, удалять уже существующих, предоставлять и отбирать различные уровни привилегий других пользователей, а также предоставление прав доступа пользователям на чужие таблицы.

Производятся попытки уничтожения уже существующих и создания новых ролей, а также предоставление и отбор привилегий пользователей на эту роль. Те же попытки производятся по отношению к представлению.

На втором этапе (см. с. 28) проводятся попытки совершения действий, зависящих от прав доступа пользователя по отношению к конкретному объекту: попытки уничтожения таблиц и других пользователей, создания и уничтожения индексов, изменения структуры таблиц, а также попытки чтения, добавления, изменения содержимого таблиц с различными правами доступа к ним.

Реализация

<u>Таблица</u>	<u>Пользователь</u>	<u>Действие</u>
	RES1	Попытка создания пользователя Axel/axelp категории CONNECT. Результат: код завершения 1022
	RES1	Попытка создания пользователя Axel/axelp категории RESOURCE. Результат: код завершения 1022

<u>Таблица</u>	<u>Пользователь</u>	<u>Действие</u>
	RES1	Попытка создания пользователя <code>Axe1/axe1p</code> категории DBA. Результат: код завершения 1022
res2.r2t1	RES1	Попытка предоставления прав доступа <code>select</code> пользователям <code>conn1</code> . Результат: код завершения 1022
res2.r2t1	RES1	Попытка предоставления прав доступа <code>select</code> пользователям <code>res1</code> . Результат: код завершения 1022
res2.r2t1	RES1	Попытка предоставления прав доступа <code>select</code> пользователям <code>res2</code> . Результат: код завершения 2152
res2.r2t1	RES1	Попытка предоставления прав доступа <code>select</code> пользователям <code>dba1</code> . Результат: код завершения 1022
	RES1	Попытка отмены привилегии RESOURCE у пользователя <code>res2</code> . Результат: код завершения 1022
res2.r2t1	RES1	Попытка отмены права <code>select</code> у пользователя <code>res2</code> . Результат: код завершения 2152
	RES1	Попытка удаления ролей <code>com_user1</code> . Результат: код завершения 1022
	RES1	Попытка удаления ролей <code>com_user2</code> . Результат: код завершения 1022
res1.r1t1	RES1	Попытка предоставления привилегий <code>insert</code> на таблицу для роли <code>com_user1</code> . Результат: операция успешна
Роль: com_user1	RES1	Попытка назначения роли пользователю <code>res2</code> . Результат: код завершения 1022
	RES1	Попытка отобрать роль <code>com_user2</code> у пользователя <code>res2</code> . Результат: код завершения 1022
	RES1	Попытка удаления пользователя <code>res1</code> . Результат: код завершения 1022
	RES1	Попытка удаления пользователя <code>conn1</code> . Результат: код завершения 1022
	RES1	Попытка изменения пароля пользователя <code>res2</code> . Результат: код завершения 1022
	RES1	Попытка уничтожения представления <code>res2.allt2</code> . Результат: код завершения 2133
res2.r2t2	RES1 (без уровня прав <code>select</code>)	Попытка выполнить <code>select</code> -запрос. Результат: код завершения 1022

<u>Таблица</u>	<u>Пользователь</u>	<u>Действие</u>
	RES1 (без уровня прав <code>select</code>)	Попытка <code>select</code> -запроса через синоним <code>res2.tab2</code> . Результат: код завершения 1022
res2.r2t2	RES1 (привилегия <code>select</code> на таблицу)	Попытка выполнить <code>insert</code> -запрос. Результат: код завершения 1022
res2.r2t2	RES1 (привилегия <code>select</code> на таблицу)	Попытка выполнить <code>update</code> -запрос. Результат: код завершения 1022
res2.r2t2	RES1 (привилегия <code>select</code> на таблицу)	Попытка выполнить <code>delete</code> -запрос. Результат: код завершения 1022
res2.r2t1	RES1 (привилегии <code>select</code> на таблицу)	Попытка изменения структуры таблицы (добавление столбца). Результат: код завершения 1022
res2.r2t2	RES1 (привилегии <code>select</code> на таблицу)	Попытка создания индекса. Результат: код завершения 1022
res2.r2t2	RES1 (привилегии <code>select</code> на таблицу)	Попытка удаления индекса. Результат: код завершения 1022
res2.r2t1	RES1 (привилегии <code>select</code> на таблицу)	Попытка удаления таблицы. Результат: код завершения 2133
res2.r2t2	RES1 (привилегия <code>select, insert</code> на таблицу)	Попытка выполнить <code>update</code> -запрос. Результат: код завершения 1022
res2.r2t2	RES1 (привилегия <code>select, insert</code> на таблицу)	Попытка выполнить <code>delete</code> -запрос. Результат: код завершения 1022
res2.r2t1	RES1 (привилегия <code>select, insert</code> на таблицу)	Попытка изменения структуры таблицы (добавление столбца). Результат: код завершения 1022
res2.r2t2	RES1 (привилегия <code>select, insert</code> на таблицу)	Попытка создания индекса. Результат: код завершения 1022
res2.r2t2	RES1 (привилегия <code>select, insert</code> на таблицу)	Попытка удаления индекса. Результат: код завершения 1022
res2.r2t1	RES1 (привилегия <code>select, insert</code> на таблицу)	Попытка удаления таблицы. Результат: код завершения 2133
res2.r2t2	RES1 (привилегия <code>select, insert, update</code> на таблицу)	Попытка выполнить <code>delete</code> -запрос. Результат: код завершения 1022

<u>Таблица</u>	<u>Пользователь</u>	<u>Действие</u>
res2.r2t1	RES1 (привилегия select, insert, update на таблицу)	Попытка изменения структуры таблицы (добавление столбца). Результат: код завершения 1022
res2.r2t2	RES1 (привилегия select, insert, update на таблицу)	Попытка создания индекса. Результат: код завершения 1022
res2.r2t2	RES1 (привилегия select, insert, update на таблицу)	Попытка удаления индекса. Результат: код завершения 1022
res2.r2t1	RES1 (привилегия select, insert, update на таблицу)	Попытка удаления таблицы. Результат: код завершения 2133
res2.r2t1	RES1 (привилегии select, insert, delete, update на таблицу)	Попытка изменения структуры таблицы (добавление столбца). Результат: код завершения 1022
res2.r2t2	RES1 (привилегии select, insert, delete, update на таблицу)	Попытка создания индекса. Результат: код завершения 1022
res2.r2t2	RES1 (привилегии select, insert, delete, update на таблицу)	Попытка удаления индекса. Результат: код завершения 1022
res2.r2t1	RES1 (привилегии select, insert, delete, update на таблицу)	Попытка удаления таблицы. Результат: код завершения 2133
res2.r2t2	RES1 (привилегии select, insert, update, delete, alter на таблицу)	Попытка создания индекса. Результат: код завершения 1022
res2.r2t2	RES1 (привилегии select, insert, update, delete, alter на таблицу)	Попытка удаления индекса. Результат: код завершения 1022
res2.r2t1	RES1 (привилегии select, insert, update, delete, alter на таблицу)	Попытка удаления таблицы. Результат: код завершения 2133

<u>Таблица</u>	<u>Пользователь</u>	<u>Действие</u>
res2.r2t1	RES1 (привилегии select, insert, update, delete, alter, index на таблицу)	Попытка удаления таблицы. Результат: код завершения 2133
res2.r2t1	RES1 (привилегии select, insert, update, delete, alter, index на таблицу)	Попытка удаления таблицы. Результат: код завершения 2133

Тестирование пользователя категории DBA

Для пользователя категории DBA на первом этапе тестируется способность предоставления прав доступа пользователям на чужие таблицы. Производятся попытки уничтожения пользователей, имеющих собственные таблицы.

На втором этапе (см. с. 31) проводятся попытки совершения действий, зависящих от прав доступа пользователя по отношению к конкретному объекту: уничтожение таблиц других пользователей, создание и уничтожение индексов, изменение структуры, а также чтение и изменение содержимого таблиц с различным доступом к ним.

Реализация

<u>Таблица</u>	<u>Пользователь</u>	<u>Действие</u>
res2.r2t1	DBA1	Попытка предоставить право select на таблицу пользователям res2 . Результат: код завершения 1022
res2.r2t1	DBA1	Попытка предоставить право select на таблицу пользователям conn1 . Результат: код завершения 1022
res2.r2t1	DBA1	Попытка предоставить право select на таблицу пользователю res2 . Результат: код завершения 2152
res2.r2t1	DBA1	Попытка отмены права delete у пользователя res2 . Результат: код завершения 2152
res2.r2t1	DBA1	Попытка отмены права delete у пользователя res1 . Результат: код завершения 1022
	DBA1	Попытка удаления пользователя SYSTEM , имеющего таблицы. Результат: код завершения 1513
	DBA1	Попытка уничтожения представления res2.allt2 . Результат: код завершения 2133
res1.r1t2	DBA1 (без уровня прав select)	Попытка выполнить select -запрос. Результат: код завершения 1022

<u>Таблица</u>	<u>Пользователь</u>	<u>Действие</u>
	DBA1 (без уровня прав <code>select</code>)	Попытка выполнить <code>select</code> -запрос через синоним <code>res1.tab1</code> . Результат: код завершения 1022
res2.r2t1	DBA1 (без уровня прав <code>select</code>)	Попытка удаления таблицы. Результат: код завершения 2133
res2.r2t2	DBA1 (без уровня прав <code>select</code>)	Попытка выполнить <code>insert</code> -запрос. Результат: код завершения 1022
res2.r2t2	DBA1 (без уровня прав <code>select</code>)	Попытка выполнить <code>update</code> -запрос. Результат: код завершения 1022
res2.r2t2	DBA1 (без уровня прав <code>select</code>)	Попытка выполнить <code>delete</code> -запрос. Результат: код завершения 1022
res2.r2t1	DBA1 (без уровня прав <code>select</code>)	Попытка изменения структуры таблицы (добавление столбца). Результат: код завершения 1022
res2.r2t1	DBA1 (без уровня прав <code>select</code>)	Попытка создания индекса. Результат: код завершения 1022
res2.r2t1	DBA1 (без уровня прав <code>select</code>)	Попытка удаления индекса. Результат: код завершения 1022
res2.r2t1	DBA1 (привилегии <code>select, insert</code> на таблицу)	Попытка удаления таблицы. Результат: код завершения 2133
res2.r2t2	DBA1 (привилегии <code>select, insert</code> на таблицу)	Попытка выполнить <code>update</code> -запрос. Результат: код завершения 1022
res2.r2t2	DBA1 (привилегии <code>select, insert</code> на таблицу)	Попытка выполнить <code>delete</code> -запрос. Результат: код завершения 1022
res2.r2t1	DBA1 (привилегии <code>select, insert</code> на таблицу)	Попытка изменения структуры таблицы (добавление столбца). Результат: код завершения 1022
res2.r2t1	DBA1 (привилегии <code>select, insert</code> на таблицу)	Попытка создания индекса. Результат: код завершения 1022
res2.r2t1	DBA1 (привилегии <code>select, insert</code> на таблицу)	Попытка удаления индекса. Результат: код завершения 1022
res2.r2t1	DBA1 (привилегии <code>select, insert, update</code> на таблицу)	Попытка удаления таблицы. Результат: код завершения 2133
res2.r2t2	DBA1 (привилегии <code>select, insert, update</code> на таблицу)	Попытка выполнить <code>delete</code> -запрос. Результат: код завершения 1022
res2.r2t1	DBA1 (привилегии <code>select, insert, update</code> на таблицу)	Попытка изменения структуры таблицы (добавление столбца). Результат: код завершения 1022

<u>Таблица</u>	<u>Пользователь</u>	<u>Действие</u>
res2.r2t1	DBA1 (привилегии select, insert, update на таблицу)	Попытка создания индекса. Результат: код завершения 1022
res2.r2t1	DBA1 (привилегии select, insert, update на таблицу)	Попытка удаления индекса. Результат: код завершения 1022
res2.r2t1	DBA1 (привилегии select, insert, update, delete на таблицу)	Попытка удаления таблицы. Результат: код завершения 2133
res2.r2t1	DBA1 (привилегии select, insert, update, delete на таблицу)	Попытка изменения структуры таблицы (добавление столбца). Результат: код завершения 1022
res2.r2t1	DBA1 (привилегии select, insert, update, delete на таблицу)	Попытка создания индекса. Результат: код завершения 1022
res2.r2t1	DBA1 (привилегии select, insert, update, delete на таблицу)	Попытка удаления индекса. Результат: код завершения 1022
res2.r2t1	DBA1 (привилегии select, insert, update, delete, alter на таблицу)	Попытка удаления таблицы. Результат: код завершения 2133
res2.r2t1	DBA1 (привилегии select, insert, update, delete, alter на таблицу)	Попытка создания индекса. Результат: код завершения 1022
res2.r2t1	DBA1 (привилегии select, insert, update, delete, alter на таблицу)	Попытка удаления индекса. Результат: код завершения 1022
res2.r2t1	DBA1 (привилегии select, insert, update, delete, alter, index на таблицу)	Попытка удаления таблицы. Результат: код завершения 2133

<u>Таблица</u>	<u>Пользователь</u>	<u>Действие</u>
res2.r2t1	DВА1 (привилегии select, insert, update, delete, alter, index, all на таблицу)	Попытка удаления таблицы. Результат: код завершения 2133

Ко второй группе тестов относится **тестирование функционирования мандатных ПРД**.

На первом этапе производятся различные действия, связанные с понятием группы: попытки создания пользователей, доступ к данным в своей и чужой группах, установки флагов доверия.

Реализация

<u>Таблица</u>	<u>Пользователь</u>	<u>Действие</u>
	RES1	Попытка создания пользователя в группе GROUP1. Результат: код завершения 1022
		Попытка создания пользователя в группе GROUP2. Результат: код завершения 1022
	DВА1	Попытка изменения своей группы пользователя RES1. Результат: код завершения 1022
		Попытка создания пользователя в группе GROUP2. Результат: код завершения 1022
		Попытка создания пользователя в группе GROUP1. Результат: успешное завершение
		Попытка создания новых уровней доступа. Результат: код завершения 1022
res2.r2t8		Попытка произвести операцию select. Результат: код завершения 1070
res2.r2t8		Попытка произвести операцию insert. Результат: код завершения 1070
res2.r2t8		Попытка произвести операцию delete. Результат: код завершения 1070
res2.r2t8		Попытка произвести операцию update. Результат: код завершения 1070
res2.r2t8		Попытка произвести операцию index. Результат: успешное завершение
res2.r2t8		Попытка произвести операцию alter. Результат: код завершения 1070
		Попытка установить флаг доверия группе GROUP1 в группе GROUP2. Результат: код завершения 1022
	RES2	Попытка установить флаг доверия группе GROUP1 в группе GROUP2. Результат: код завершения 1022

<u>Таблица</u>	<u>Пользователь</u>	<u>Действие</u>
	DVA2	Попытка установить флаг доверия группе GROUP1. Результат: успешное завершение
	DVA1	Попытка установить флаг доверия группе GROUP2. Результат: успешное завершение

На втором этапе производятся различные действия, связанные с понятием уровней доступа: создание информации с неверными уровнями доступа, чтение запрещенной информации и т.д.

Ошибки в ответах могут возникать в результате попытки работать с таблицами (столбцами), уровни доступа которых жестче уровней доступа пользователя или при указании неверных уровней доступа в процессе создания новых записей. Если доступ к таблице (столбцу) разрешен, то результатом **select**, **update** или **delete**-запроса будет количество обработанных строк. Запрет доступа на уровне записи (поля записи) приводит к тому, что эта запись не будет обрабатываться. В результате ответ может содержать количество обработанных записей 0 даже в случае наличия удовлетворяющих запросу записей.

При запросе **alter table** ошибка возникает в случае, если метка чтения пользователя меньше метки чтения или записи таблицы или указании неверных уровней доступа к создаваемому столбцу.

Группа тестов, связанная с созданием таблиц с различными уровнями доступа, изменения уровней доступа пользователей.

Реализация

<u>Таблица</u>	<u>Пользователь</u>	<u>Действие</u>
	DVA1	Попытка создания таблицы d1t1. Результат: успешное завершение
	DVA1	Попытка создания таблицы d1t2 с R=6, W=6. Результат: успешное завершение
	DVA1	Попытка создания таблицы d1t3 с R=3 W=3. Результат: код завершения 1022
	DVA1	Попытка создания таблицы d1t4 с уровнем доступа к отдельному столбцу R=3 W=3. Результат: код завершения 1022
	DVA1	Попытка изменения уровней доступа пользователя RES1 (R=6, W=5). Результат: код завершения 1022
	DVA1	Попытка изменения уровней доступа пользователя RES1 (R=5, W=4). Результат: код завершения 1022
	DVA1	Попытка изменения уровней доступа пользователя RES1 (R=4, W=6). Результат: успешное завершение
	SYSTEM	Попытка изменения уровней доступа пользователя RES1 (R=6, W=5). Результат: успешное завершение

<u>Таблица</u>	<u>Пользователь</u>	<u>Действие</u>
	DBA1	Попытка изменения уровней доступа пользователя RES1 (R=5, w=4). Результат: успешное завершение
	SYSTEM	Попытка изменения уровней доступа пользователя RES1 (R=4, w=6). Результат: успешное завершение
res2.r2t1	DBA1	Попытка произвести <code>select * ...</code> при <code>PersID=2</code> . Результат: возвращаются 2 строки;
res2.r2t2	DBA1	Попытка произвести <code>select * ...</code> . Результат: возвращаются 3 строки
res2.r2t3	DBA1	Попытка произвести <code>select * ...</code> . Результат: ошибка 1070
res2.r2t4	DBA1	Попытка произвести <code>select * ...</code> . Результат: код завершения 1070
res2.r2t5	DBA1	Попытка произвести <code>select * ...</code> . Результат: код завершения 1070
res2.r2t5	DBA1	Попытка произвести <code>select model5 ...</code> . Результат: код завершения 1070
res2.r2t5	DBA1	Попытка произвести <code>select PersId ...</code> . Результат: возвращаются 3 строки
res2.r2t6	DBA1	Попытка произвести <code>select * ...</code> . Результат: возвращаются 3 строки
res2.r2t7	DBA1	Попытка произвести <code>select * ...</code> . Результат: код завершения 1070
res2.r2t7	DBA1	Попытка произвести <code>select model7 ...</code> . Результат: код завершения 1070
res2.r2t1	DBA1	Попытка произвести <code>select * ...</code> при <code>PersID=1</code> . Результат: возвращаются 2 строки
res2.r2t1	DBA1	Попытка произвести <code>select model1 ...</code> при <code>PersID=1</code> . Результат: возвращаются 2 строки
res2.r2t1	DBA1	Попытка произвести <code>insert</code> . Результат: успешное завершение
res2.r2t2	DBA1	Попытка произвести <code>insert</code> . Результат: код завершения 1070
res2.r2t3	DBA1	Попытка произвести <code>insert</code> . Результат: успешное завершение
res2.r2t4	DBA1	Попытка произвести <code>insert</code> . Результат: код завершения 1070
res2.r2t5	DBA1	Попытка произвести <code>insert</code> . Результат: код завершения 1070
res2.r2t5	DBA1	Попытка произвести <code>insert</code> в поле <code>PersId</code> . Результат: успешное завершение

Таблица	Пользователь	Действие
res2.r2t6	DBA1	Попытка произвести <code>insert</code> . Результат: код завершения 1070
res2.r2t7	DBA1	Попытка произвести <code>insert</code> . Результат: успешное завершение
res2.r2t1	DBA1	Попытка произвести <code>insert</code> с R=3 для записи. Результат: код завершения 1070
res2.r2t1	DBA1	Попытка произвести <code>insert</code> с R=3 для поля <code>Model1</code> . Результат: код завершения 1070
res2.r2t1	DBA1	Попытка произвести <code>insert</code> с R=6, W=6 для записи. Результат: успешное завершение
res2.r2t1	DBA1	Попытка произвести <code>insert</code> с R=6, W=6 для поля <code>Model1</code> . Результат: успешное завершение
res2.r2t1	DBA1	Попытка произвести <code>update</code> при <code>PersID=2</code> . Результат: изменяется одна строка;
res2.r2t1	DBA1	Попытка произвести <code>update</code> при <code>PersID=1</code> . Результат: изменяется одна строка
res2.r2t2	DBA1	Попытка произвести <code>update</code> . Результат: код завершения 1070
res2.r2t3	DBA1	Попытка произвести <code>update</code> . Результат: код завершения 1070
res2.r2t4	DBA1	Попытка произвести <code>update</code> . Результат: код завершения 1070
res2.r2t5	DBA1	Попытка произвести <code>update</code> . Результат: код завершения 1070
res2.r2t5	DBA1	Попытка произвести <code>update</code> столбца <code>PersId</code> . Результат: изменяются 4 строки
res2.r2t6	DBA1	Попытка произвести <code>update</code> . Результат: код завершения 1070
res2.r2t7	DBA1	Попытка произвести <code>update</code> . Результат: код завершения 1070
res2.r2t5	DBA1	Попытка произвести <code>update</code> столбца <code>Make</code> . Результат: изменяются 3 строки
res2.r2t6	DBA1	Попытка произвести <code>update</code> столбца <code>Make</code> . Результат: изменяются 3 строки
res2.r2t7	DBA1	Попытка произвести <code>update</code> столбца <code>Make</code> . Результат: изменяются 3 строки
res2.r2t1	DBA1	Попытка произвести <code>update</code> поля <code>Model1</code> (R=6) всех строк с <code>PersID=10</code> . Результат: изменяется одна строка
res2.r2t1	DBA1	Попытка произвести <code>update</code> поля <code>Model1</code> (R=3) всех строк с <code>PersID=10</code> . Результат: код завершения 1070
res2.r2t1	DBA1	Попытка произвести <code>delete</code> с <code>PersID=1</code> . Результат: удалена одна строка

<u>Таблица</u>	<u>Пользователь</u>	<u>Действие</u>
res2.r2t1	DVA1	Попытка произвести <code>delete</code> с <code>PersID=2</code> . Результат: удалена одна строка
res2.r2t2	DVA1	Попытка произвести <code>delete</code> . Результат: код завершения 1070
res2.r2t3	DVA1	Попытка произвести <code>delete</code> . Результат: код завершения 1070
res2.r2t4	DVA1	Попытка произвести <code>delete</code> . Результат: код завершения 1070
res2.r2t5	DVA1	Попытка произвести <code>delete</code> всех записей. Результат: код завершения 1070
res2.r2t6	DVA1	Попытка произвести <code>delete</code> всех записей. Результат: код завершения 1070
res2.r2t7	DVA1	Попытка произвести <code>delete</code> всех записей. Результат: код завершения 1070
res2.r2t4	DVA1	Попытка произвести <code>alter</code> . Результат: код завершения 1070
res2.r2t1	DVA1	Попытка произвести <code>alter</code> . Результат: успешное завершение

Идентификация и аутентификация

Успешное осуществление идентификации и аутентификации пользователя неявно проверяется во время тестирования дискреционных и мандатных ПРД. Все тесты осуществляются зарегистрированными пользователями. Если во время регистрации произошла ошибка, выполнение теста прерывается, выдается соответствующее сообщение.

Контроль целостности КСЗ

Для контроля целостности КСЗ используется задача `count`, вычисляющая контрольную сумму исполняемого кода ядра.

Тестирование производится путем небольшого видоизменения исполняемого кода ядра с последующим вычислением контрольной суммы. Результатом является несовпадение контрольных сумм до и после видоизменения. Это говорит о том, что произошло нарушение целостности КСЗ.

Маркировка документов

Получить данные из СУБД ЛИНТЕР можно только посредством SQL-запросов. Для маркировки документов, составляемых из этих данных, предусмотрена возможность получения максимального уровня конфиденциальности (уровня доступа `GROUP`, `RAL`, `WAL`) информации, полученной с помощью SQL-запроса.

Для тестирования создается таблица из 7 записей со следующими метками доступа:

№ строки	Группа	RAL	WAL
1	1	4	4
2	1	4	5
3	1	4	6
4	1	5	4

5	1	5	5
6	1	5	6
7	1	6	6

Записи этой таблицы обладают различными уровнями конфиденциальности. Производится Select-запрос. Проверяется возможность получения метки уровня конфиденциальности.

Результатом теста является выдача на экран всех записей и уровней конфиденциальности (GROUP, RAL, WAL) каждой из них:

```

Creating of user's groups ;...
Creating of security level's ...
ID          | Model   | Make   | Level's
-----
1           | ford1   | 1984   | G=1 R=4 W=4
2           | ford2   | 1985   | G=1 R=4 W=5
3           | ford3   | 1986   | G=1 R=4 W=6
4           | ford4   | 1987   | G=1 R=5 W=4
5           | ford5   | 1988   | G=1 R=5 W=5
6           | ford6   | 1989   | G=1 R=5 W=6
7           | ford7   | 1990   | G=1 R=6 W=6
Maximum group level (G) : 1
Maximum read level (R) : 6
Maximum write level (W) : 6
    
```

Тест подтверждает возможность получения информации о наибольшем уровне секретности выбранных данных для формирования меток для маркировки документов.

Механизм надежного восстановления

Механизм надежного восстановления обеспечивается СУБД ЛИНТЕР. Его основой является ведение системного журнала, в котором отображаются все изменения, которые производятся с БД всеми пользователями системы. Все действия, связанные с изменениями в системе защиты, также отображаются в журнале (создание/удаление нового пользователя/группы и т.д.). Если пользователь получил уведомление о том, что его изменения перенесены в БД, то сбой оборудования не может привести к нарушению системы защиты.

Реализация

- 1) моделируется отказ оборудования в момент работы ядра СУБД (например, путем выключения электропитания на компьютере);
- 2) после перезапуска операционной системы и проведения процедуры запуска СУБД ЛИНТЕР можно провести стандартное испытание (в соответствии с настоящим документом) механизмов КСЗ и убедиться в полном восстановлении свойств КСЗ СУБД ЛИНТЕР.

Регистрация событий

Проверяется тестами audtest1 и audtest2.

Тестирование заключается в совершении над системой некоторого действия, подлежащего регистрации, с последующей проверкой наличия записи об этом событии в таблице \$\$\$AUDIT.

Реализация

- 1) первоначально запускается тест `audtest1 - auditstart`, который иницирует в СУБД систему регистрации событий и разрешает регистрацию только двух событий: старта и останова СУБД ЛИНТЕР;
- 2) ядро СУБД ЛИНТЕР завершается (подается команда `SHUT`);
- 3) ядро СУБД ЛИНТЕР запускается снова;
- 4) запускается тест `audtest2 - check`, который производит выборку из таблицы `$$$AUDIT`, проверяя наличие в ней информации о событии - завершении ядра СУБД и о событии - старте ядра СУБД и останавливает систему регистрации.

`Audtest2` включает систему регистрации и разрешает регистрацию всех событий, необходимых для тестирования. Далее тест генерирует события и проверяет их регистрацию в БД. События 3-6 (см. ниже) могут быть протестированы только при первом запуске утилиты `audtest2` на данной БД. При необходимости повторного тестирования этих событий нужно пересоздать БД.

<u>Номер события</u>	<u>Событие</u>	<u>Результат</u>
1	Регистрация пользователя	Успешная регистрация
2	Запуск системы регистрации	Успешная регистрация
3	Создание группы	Успешная регистрация
4	Изменение имени группы	Успешная регистрация
5	Создание уровня	Успешная регистрация
6	Изменение имени уровня	Успешная регистрация
7	Создание пользователя	Успешная регистрация
8	Изменение категории пользователя	Успешная регистрация
9	Разрешение доступа к группе	Успешная регистрация
10	Создание роли	Успешная регистрация
11	Назначение роли	Успешная регистрация
12	Отмена назначения роли	Успешная регистрация
13	Удаление роли	Успешная регистрация
14	Создание таблицы	Успешная регистрация
15	Передача пользователю DBA1 права на SELECT для созданной в событии 14 таблицы	Успешная регистрация
16	Передача пользователю DBA1 права на INSERT для созданной в событии 14 таблицы	Успешная регистрация
17	Передача пользователю DBA1 права на UPDATE для созданной в событии 14 таблицы	Успешная регистрация

<u>Номер события</u>	<u>Событие</u>	<u>Результат</u>
18	Передача пользователю DBA1 права на DELETE для созданной в событии 14 таблицы	Успешная регистрация
19	Передача пользователю DBA1 права на ALTER для созданной в событии 14 таблицы	Успешная регистрация
20	Передача пользователю DBA1 права на INDEX для созданной в событии 14 таблицы	Успешная регистрация
21	Передача пользователю DBA1 всех прав на созданную в событии 14 таблицу	Успешная регистрация
22	Создание индекса	Успешная регистрация
23	Удаление индекса	Успешная регистрация
24	Назначение привилегий на таблицу	Успешная регистрация
25	Создание синонима	Успешная регистрация
26	Удаление синонима	Успешная регистрация
27	Занесение строки в таблицу	Успешная регистрация
28	Выборка из таблицы	Успешная регистрация
29	Изменение строк в таблице	Успешная регистрация
30	Создание представления	Успешная регистрация
31	Удаление представления	Успешная регистрация
32	Удаление строк из таблицы	Успешная регистрация
33	Попытка доступа к БД (регистрации) незарегистрированного в ней пользователя	Запись в таблице \$\$\$AUDIT о попытке регистрации недопустимого пользователя
34	Изменение пароля пользователя	Успешная регистрация
35	Удаление таблицы	Успешная регистрация
36	Отмена разрешения доступа к группе	Успешная регистрация
37	Удаление пользователя	Успешная регистрация
38	Останов системы регистрации	Успешная регистрация

Сопоставление пользователя с устройством и защита физических устройств


Проверяется тестами device, stations, userconn.

Тест device проверяет реализацию физических устройств в структуре БД.

Тест stations проверяет реализации сетевых устройств.

Реализация теста device

- 1) Соединение администратора безопасности (далее «администратор») с сервером ЛИНТЕР и создание пользователя USER1 в группе GR1 с правами RESOURCE. Предполагается, что с данной рабочей станции пользователям группы GR1 (\$\$ID=1) разрешен доступ к серверу ЛИНТЕР.
- 2) Соединение с ЛИНТЕР пользователя USER1/USER1.

 В случае возникновения ошибок соединения с сервером ЛИНТЕР, создания пользователя, выдачи привилегий работа теста завершается с выдачей соответствующего сообщения;

- 3) Попытка пользователя USER1 создать устройство DV01, если она успешна, то последует завершение теста с сообщением об ошибке.
- 4) Создание администратором устройства DV01 с уровнями <RAL,WAL>=<"LEV10", "LEV10">, в случае возникновения ошибки последует завершение теста с сообщением об ошибке.
- 5) Попытка создания администратором устройства DV01 (то есть дубликата) с уровнями <RAL,WAL>=<"LEV10", "LEV10">, в случае успеха последует завершение теста с сообщением об ошибке.
- 6) Попытка пользователя USER1 создать на DV01 таблицу ZZ с <RAL,WAL>=<"LEV10", "LEV10">, в случае успеха тест завершается с сообщением об ошибке.
- 7) Изменение администратором уровня пользователя USER1 на <RAL,WAL>=<"LEV10", "LEV10">.
- 8) Попытка пользователя USER1 создать на DV01 таблицу ZZ с <RAL,WAL>=<"LEV10", "LEV10">, в случае неуспеха тест завершается с сообщением об ошибке.
- 9) Разрушение таблицы ZZ, в случае неуспеха тест завершается с сообщением об ошибке.
- 10) Изменение администратором уровня пользователя USER1 на <RAL,WAL>=<"LEV1", "LEV1">.
- 11) Попытка пользователя USER1 создать на DV01 таблицу ZZ с <RAL,WAL>=<"LEV10", "LEV10">, в случае успеха тест завершается с сообщением об ошибке.
- 12) Попытка пользователя USER1 уничтожить устройство DV01, в случае успеха следует завершение теста с сообщением об ошибке;
- 13) Изменение администратором уровня пользователя USER1 на <RAL,WAL>=<"LEV10", "LEV10">.
- 14) Попытка разрушения таблицы ZZ, в случае неуспеха тест завершается с сообщением об ошибке.
- 15) Попытка пользователя USER1 уничтожить устройство DV01, в случае успеха следует завершение теста с сообщением об ошибке.
- 16) Уничтожение устройства DV01 администратором, в случае неуспеха тест завершается с сообщением об ошибке.
- 17) Создание администратором устройства DV01 с уровнями <RAL,WAL>=<"LEV2", "LEV2">, в случае возникновения ошибки последует завершение теста с сообщением об ошибке.
- 18) Попытка создания администратором устройства DV01 (то есть дубликата) с уровнями <RAL,WAL>=<"LEV8", "LEV8">, в случае успеха последует завершение теста с сообщением об ошибке.


- 19) Уничтожение устройства DV01 администратором, в случае неуспеха тест завершается с сообщением об ошибке.
- 20) Создание администратором устройства DV01 с уровнями <RAL,WAL>=<"LEV8", "LEV8">, в случае возникновения ошибки последует завершение теста с сообщением об ошибке.
- 21) Попытка создания администратором устройства DV01 (то есть дубликата) с уровнями <RAL,WAL>=<"LEV2", "LEV2">, в случае успеха последует завершение теста с сообщением об ошибке.
- 22) Уничтожение устройства DV01 администратором, в случае неуспеха тест завершается с сообщением об ошибке.
- 23) Создание администратором устройства DV01 с уровнями <RAL,WAL>=<"LEV8", "LEV8">, в случае возникновения ошибки последует завершение теста с сообщением об ошибке.
- 24) Изменение администратором уровня DV01 на <RAL,WAL>=<"LEV4", "LEV4">, в случае возникновения ошибки последует завершение теста с сообщением об ошибке.
- 25) Изменение администратором уровня пользователя USER1 на <RAL,WAL>=<"LEV2", "LEV2">, в случае возникновения ошибки последует завершение теста с сообщением об ошибке.
- 26) Попытка пользователя USER1 изменить уровень устройства DV01 на <RAL,WAL>=<"LEV2", "LEV2">, в случае успеха последует завершение теста с сообщением об ошибке.
- 27) Уничтожение устройства DV01 администратором, в случае неуспеха тест завершается с сообщением об ошибке.
- 28) Создание администратором устройства DV01 с уровнями <RAL,WAL>=<"LEV8", "LEV8">, в случае возникновения ошибки последует завершение теста с сообщением об ошибке.
- 29) Изменение администратором уровня пользователя USER1 на <RAL,WAL>=<"LEV8", "LEV4">, в случае возникновения ошибки последует завершение теста с сообщением об ошибке.
- 30) Создание пользователем USER1 на DV01 таблицы ZZ с <RAL,WAL>=<"LEV8", "LEV8">, в случае возникновения ошибки последует завершение теста с сообщением об ошибке.
- 31) Попытка разрушения пользователем USER1 таблицы ZZ, в случае неуспеха тест завершается с сообщением об ошибке.
- 32) Изменение администратором уровня DV01 на <RAL,WAL>=<"LEV8", "LEV4">, в случае неуспеха последует завершение теста с сообщением об ошибке.
- 33) Попытка разрушения пользователем USER1 таблицы ZZ, в случае неуспеха тест завершается с сообщением об ошибке.
- 34) Изменение администратором уровня DV01 на <RAL,WAL>=<"LEV9", "LEV9">, в случае неуспеха последует завершение теста с сообщением об ошибке.
- 35) Попытка создания пользователем USER1 на DV01 таблицы ZZ с <RAL,WAL>=<"LEV9", "LEV9">, в случае успеха последует завершение теста с сообщением об ошибке.
- 36) Изменение администратором уровня пользователя на <RAL,WAL>=<"LEV9", "LEV9">, в случае неуспеха последует завершение теста с сообщением об ошибке.
- 37) Попытка разрушения ZZ. В случае неуспеха последует сообщение об ошибке.
- 38) Уничтожение устройства DV01 администратором, в случае неуспеха тест завершается с сообщением об ошибке.
- 39) Создание администратором устройства DV01 с уровнями <RAL,WAL>=<"LEV8", "LEV8">, в случае возникновения ошибки последует завершение теста с сообщением об ошибке.

- 40) Изменение администратором уровня пользователя **USER1** на `<RAL,WAL>=<"LEV8", "LEV8">`, в случае возникновения ошибки последует завершение теста с сообщением об ошибке.
- 41) Создание пользователем **USER1** таблицы **ZZ** на **DV01** с `<RAL,WAL>=<"LEV8", "LEV8">`, в случае возникновения ошибки последует завершение теста с сообщением об ошибке.
- 42) Администратор разрешает доступ к **DV01** группам **GR2** и **GR3** и запрещает доступ к **DV01** группе **GR1**.
- 43) Попытка пользователя **USER1** добавить запись в **ZZ** на **DV01**, в случае успеха тест завершается с сообщением об ошибке.
- 44) Перевод администратором пользователя **USER1** из **GR1** в **GR2**.
- 45) Попытка пользователя **USER1** добавить запись в **ZZ** на **DV01**, в случае неуспеха тест завершается с сообщением об ошибке.
- 46) Администратор запрещает доступ к **DV01** группе **GR2**.
- 47) Попытка пользователя **USER1** добавить запись в **ZZ** на **DV01**, в случае успеха тест завершается с сообщением об ошибке.
- 48) Администратор разрешает доступ к **DV01** всем (**ALL**).
- 49) Попытка пользователя **USER1** добавить запись в **ZZ** на **DV01**, в случае неуспеха тест завершается с сообщением об ошибке.
- 50) Администратор запрещает доступ к **DV01** всем (**ALL**).
- 51) Попытка пользователя **USER1** добавить запись в **ZZ** на **DV01**, в случае успеха тест завершается с сообщением об ошибке.
- 52) Администратор разрешает доступ к **DV01** группе **GR2**.
- 53) Попытка пользователя **USER1** добавить запись в **ZZ** на **DV01**, в случае неуспеха тест завершается с сообщением об ошибке.
- 54) Разрушение пользователем **USER1** таблицы **ZZ** на **DV01**, в случае неуспеха тест завершается с сообщением об ошибке.
- 55) Уничтожение устройства **DV01** администратором, в случае неуспеха тест завершается с сообщением об ошибке.

Номера действий теста `userconn` согласованы с номерами действий теста `stations`. Действия 1-3 выполняются только в тесте `stations`, нумерация действий для теста `userconn` начинается с действия 4.

Реализация теста `stations` и `userconn`

- 1) Соединение администратора безопасности с сервером **ЛИНТЕР** и создание пользователя **USER1** в группе **GR1** с правами **RESOURCE**. Предполагается, что с данной рабочей станции пользователям группы **GR1** (`$$$ID=1`) разрешен доступ к серверу **ЛИНТЕР**.
- 2) Соединение с СУБД **ЛИНТЕР** пользователя **USER1/USER1**.

 В случае возникновения ошибок соединения с сервером **ЛИНТЕР**, создания пользователя, выдачи привилегий последует завершение теста с соответствующим сообщением об ошибке.

- 3) Соединение пользователя **USER1** с сервером **ЛИНТЕР**.
- 4) Попытка пользователя **USER1** создать станцию (далее условно - **COMPUTERNAME**), если она успешна, то последует завершение теста с сообщением об ошибке.
- 5) Создание администратором станции **COMPUTERNAME**, в случае возникновения ошибки последует завершение теста с сообщением об ошибке.
- 6) Попытка создания администратором станции **COMPUTERNAME** (то есть дубликата), в случае успеха последует завершение теста с сообщением об ошибке.
- 7) Запуск `userconn /local` (значения параметров `/USER`, `/PASSWORD` тестов `stations` и `userconn` должны совпадать), в случае успеха тест завершится сообщением `test passed`.

- 8) Запуск userconn со станции COMPUTERNAME (без ключа /local, значения параметров /USER, /PASSWORD тестов stations и userconn должны совпадать).
- 9) Тест stations изменяет права доступа пользователей со станции COMPUTERNAME для пользователя USER1, а тест userconn проверяет возможность соединения и операций с данными на сервере ЛИНТЕР. Об успешном завершении теста свидетельствует сообщение:
test <номер теста> passed, press any key to start next test
- 10) Запрещение администратором соединения с ЛИНТЕР со станции COMPUTERNAME. Старт действия 4 userconn. Об успешном завершении теста свидетельствует сообщение:
test <номер теста> passed, press any key to start next test
- 11) Разрешение администратором соединения с ЛИНТЕР со станции COMPUTERNAME. Старт действия userconn. Об успешном завершении теста свидетельствует сообщение:
test <номер теста> passed, press any key to start next test
- 12) Запрещение администратором соединения с ЛИНТЕР со станции COMPUTERNAME группе GR1. Старт действия 6 userconn. Об успешном завершении теста свидетельствует сообщение:
test <номер теста> passed, press any key to start next test
- 13) Перевод администратором пользователя USER1 из группы GR1 в группу GR2, разрешение администратором соединения с ЛИНТЕР со станции COMPUTERNAME группе GR2. Старт действия 7 userconn. Об успешном завершении теста свидетельствует сообщение:
test <номер теста> passed, press any key to start next test
- 14) Разрешение администратором соединения с ЛИНТЕР со станции COMPUTERNAME группе GR2, изменение уровня станции на <RAL,WAL>=<"LEV10", "LEV10">, изменение уровня пользователя USER1 на <RAL,WAL>=<"LEV10", "LEV10">. Старт действия 8 userconn. Об успешном завершении теста (успешное соединение и операции с данными) свидетельствует сообщение:
test <номер теста> passed, press any key to start next test
- 15) Разрешение администратором соединения с ЛИНТЕР со станции COMPUTERNAME группе GR2, изменение уровня станции на <RAL,WAL>=<"LEV10", "LEV10">, изменение уровня пользователя USER1 на <RAL,WAL>=<"LEV2", "LEV2">. Старт действия 9 userconn. Об успешном завершении теста свидетельствует сообщение:
test <номер теста> passed, press any key to start next test
- 16) Разрешение администратором соединения с ЛИНТЕР со станции COMPUTERNAME группе GR2, изменение уровня станции на <RAL,WAL>=<"LEV6", "LEV4">, изменение уровня пользователя USER1 на <RAL,WAL>=<"LEV7", "LEV10">. Старт действия 10 userconn. Об успешном завершении теста (успешное соединение и операции с данными) свидетельствует сообщение:
test <номер теста> passed, press any key to start next test
- 17) Разрешение администратором соединения с ЛИНТЕР со станции COMPUTERNAME группе GR2, изменение уровня станции на <RAL,WAL>=<"LEV6", "LEV4">, изменение уровня пользователя USER1 на <RAL,WAL>=<"LEV4", "LEV4">.

Старт действия 11 userconn. Об успешном завершении теста свидетельствует сообщение:

```
test <номер теста> passed, press any key to start next test
```

Контроль дистрибуции программных средств

Проверяется тестом count.

Каждый дистрибутивный комплект программных средств, составляющих СУБД ЛИНТЕР, должен тестироваться на соответствие эталонному образцу. Для реализации этой задачи используется механизм вычисления контрольной суммы как для всех файлов, входящих в дистрибутивный комплект, так и для всего комплекта сразу. Для вычисления значений контрольных сумм предназначена специальная утилита, описываемая ниже.

Для контроля точности копирования при изготовлении копий с образца дистрибутивного комплекта программных средств СУБД ЛИНТЕР необходимо непосредственно перед установкой системы произвести вычисление контрольной суммы. В случае полного соответствия, дистрибутивная копия программных средств считается повторяющей образец.

Разработчик может производить изменения в исходных текстах программ, приводящие к изменению исполняемых модулей, входящих в дистрибутивный комплект. Изменения документируются, и эталонное значение контрольной суммы дистрибутивного комплекта пересчитывается.

Пользователь комплекса программных средств СУБД ЛИНТЕР должен информировать разработчиков о каждом случае несовпадения контрольной суммы дистрибутивного комплекта и эталонного значения.

Для контроля точности копирования при изготовлении дистрибутивных копий комплекса программных средств СУБД ЛИНТЕР используется специальная утилита count:

Реализация теста

Для указанного файла производится расчет 16-байтной последовательности символов, однозначно идентифицирующих заданный файл. Расчет производится с использованием распространенного алгоритма вычисления *аутентифицирующих кодов Message Digest* в режиме сцепления по промежуточному результату вычислений.

Правила использования дистрибуции:

- получить дубль эталонных носителей системы на других носителях для запасного варианта хранения. Данная операция производится стандартными утилитами копирования файлов соответствующей операционной системы или путем записи специальными программами на CD-диск. Возможно выполнение копии с промежуточным копированием с дистрибутивного диска на локальный диск;
- записать дистрибутив на дублирующий носитель;
- сравнить эталонные и дублирующие носители с помощью процедуры контроля дистрибуции;
- дублирующие носители необходимо сохранить с теми же правилами предосторожности, что и эталонные;

- если необходимо использовать дубль системы, этот дубль предварительно следует проверить при помощи процедуры контроля дистрибуции (сверив контрольные суммы дубля с эталонными);
- охрана программ должна быть реализована с помощью организационных и административных мер безопасности.

