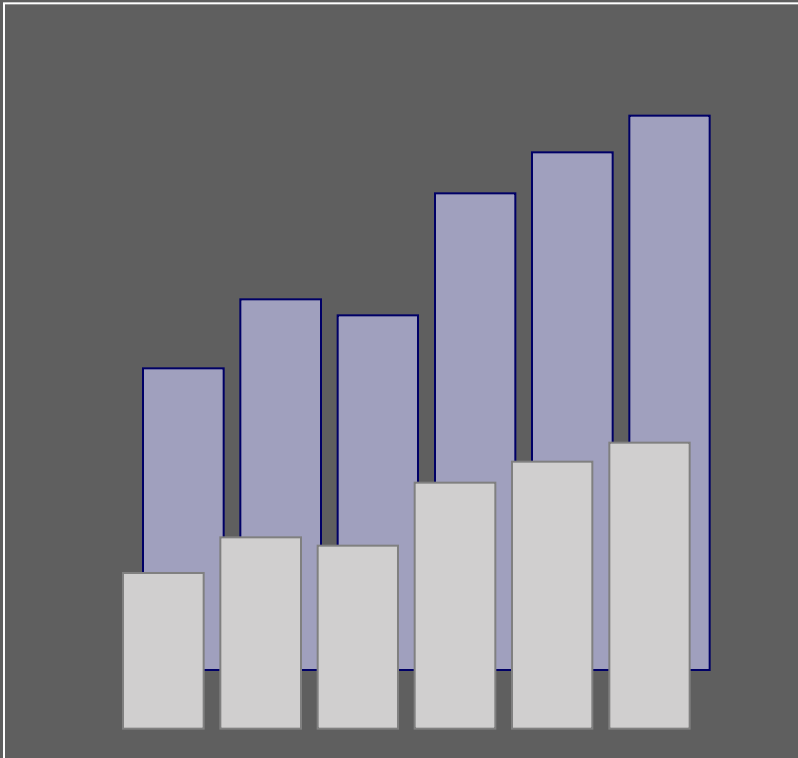


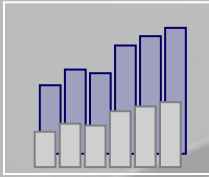
# Transparent Data Encryption OpenEdge 10.2B



Башкатов В.Г.  
v.bashkatov@csbi.ru  
www.openedge.ru



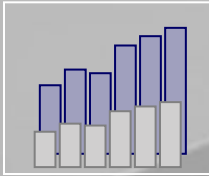
# Зачем необходимо шифрование базы данных?



- ✓ **Защита бизнеса** (примерно 65% компаний становятся банкротами вследствие утраты 20% служебной информации)
- ✓ **Соблюдение законов**



# Зачем необходимо шифрование базы данных?



The screenshot shows a Google search results page for the query "Украдена база данных". The search results are as follows:

- Украдена база данных 3 тыс. школьных сотрудников - Информационная ...**  
17 окт 2008 ... Информационная безопасность: персональные данные, США, Алексей Доля, Perimetrix, ФСТЭК, инсайдеры, шифрование, ЭЦП.  
[www.itsec.ru/newstext.php?news...](http://www.itsec.ru/newstext.php?news...) - Сохранено в кэше - Похожие
- Украдена база данных 3 тыс. школьных сотрудников - PCNEWS.RU**  
Все компьютерные новости на PCNews.ru. Вся новая информация, о компьютерах и информационных технологиях. Синдикация новостей, статей, пресс-релизов со всех ...  
[www.pcnews.ru/.../17-steven-brown-50-fort-wayne-perimetrix-245878.html](http://www.pcnews.ru/.../17-steven-brown-50-fort-wayne-perimetrix-245878.html) - Сохранено в кэше - Похожие
- Украдена база данных по кредитам россиян**  
Форум журнала «Хакер»: самый популярный форум для хакеров, взломщиков, администраторов.  
[forum.haker.ru/m.../tm.htm](http://forum.haker.ru/m.../tm.htm) - Сохранено в кэше - Похожие
- Би-би-си | Технологии | Украдена база данных абонентов "МТС"**  
Украдена абонентская база данных крупнейшего российского оператора мобильной связи "МТС". Пиратские компакт-диск с личными сведениями продаются на рынках ...  
[news.bbc.co.uk/.../2662141.stm](http://news.bbc.co.uk/.../2662141.stm) - Сохранено в кэше - Похожие
- Украдена база МТС**  
Украдена база МТС Персональная информация стала в России ходовым товаром. Сообщения о том, что база данных об абонентах "Мобильных ТелеСистем" появилась на ...  
[www.aboutstudy.ru/news.php?id...](http://www.aboutstudy.ru/news.php?id...) - Сохранено в кэше - Похожие
- В Херсоне украдена база Партии Регионов! | ХайВей**  
11 июл 2009 ... По словам Андрея Заднипряного никакого хищения не было, картотека партии и системный блок ПК с базой данных района не украдены, ...  
[h.ua/story/212598/](http://h.ua/story/212598/) - Сохранено в кэше - Похожие
- Хакер Online -> Украдена база данных по кредитам россиянам**  
16 авг 2006 ... Сайт журнала «Хакер»: самый авторитетный ресурс рунета, посвященный вопросам информационной безопасности. Украдена база данных по кредитам ...  
[www.haker.ru/post/.../default.asp](http://www.haker.ru/post/.../default.asp) - Сохранено в кэше - Похожие
- ИноСМИ.Ru | Украдены данные на шесть миллионов абонентов мобильной ...**  
Эта база данных, в которой имеются также сведения на политических деятелей и бизнесменов, была украдена из МТС, самой крупной в России сети мобильной ...  
[www.inosmi.ru/.../169905.html](http://www.inosmi.ru/.../169905.html) - Сохранено в кэше - Похожие
- Украдена база пользователей «ВКонтакте» - AmiGator Web Site**  
Вчера в свободный доступ попала база данных нескольких десятков тысяч пользователей ВКонтакте. ... Украдена база пользователей «ВКонтакте». 31.07.2009 18:09

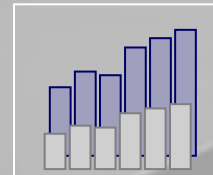
Рекламные ссылки:

- 300 млн номеров в базе**  
Пеленгатор нового поколения  
Точное местонахождение абонента  
[radar2009.ru](http://radar2009.ru)
- Пробей человека по базе**  
Новый уникальный онлайн-проект.  
Мы знаем все о каждом!  
[po-baze.ru](http://po-baze.ru)
- Интернет-шпион**  
Осуществляет поиск по огромному количеству интернет-источников  
[internet-shpion.ru](http://internet-shpion.ru)

[Разместите здесь свою рекламу >](#)



# Что такое TDE?



## 1. Прозрачность

- Без изменения приложения
- Без перезагрузки данных

## 2. Гибкость

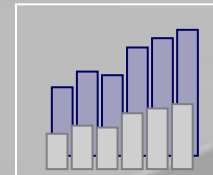
- Шифрование конкретный объектов в области SAT-II
- Шифрование конкретной области SAT-I
- Шифрование блоков на диске

## 3. Безопасность

- Поддержка хранилища ключей
- Ограниченный доступ к физическим данным
- Часть стратегии безопасности



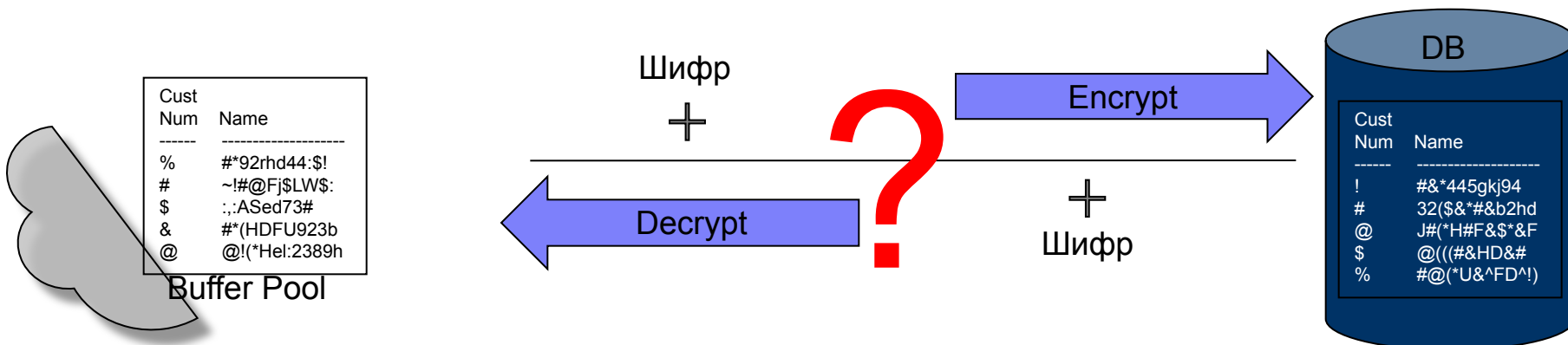
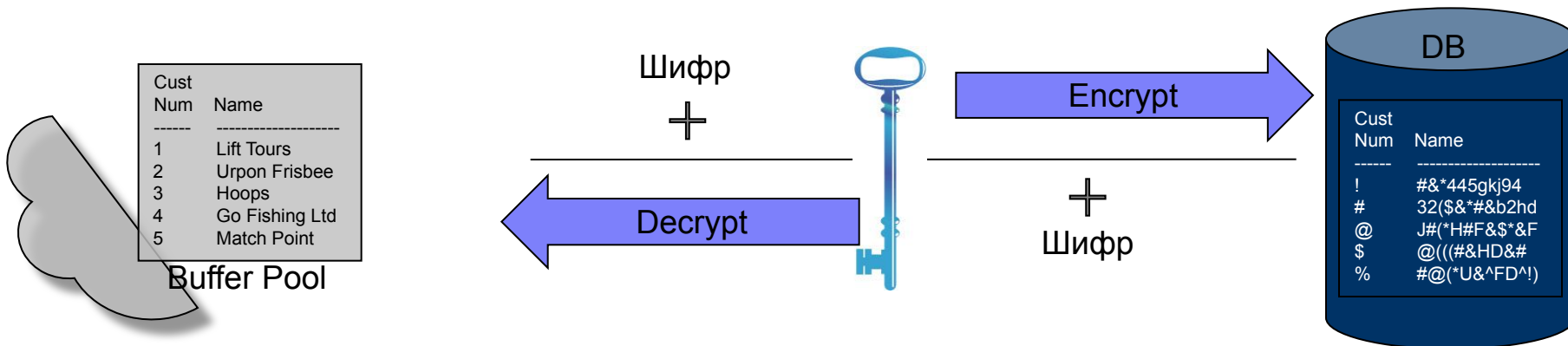
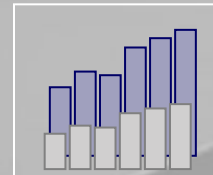
## OpenEdge TDE:



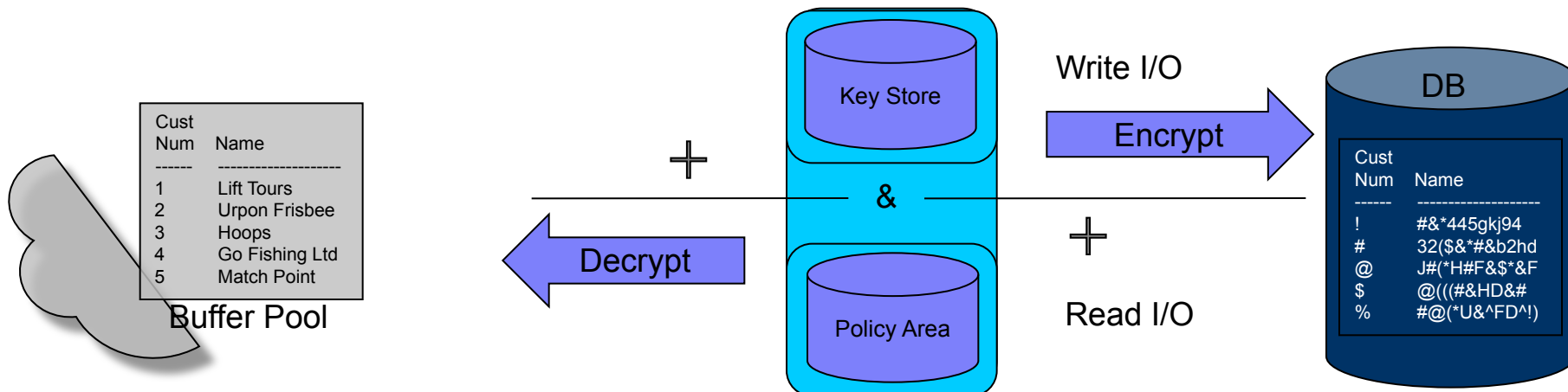
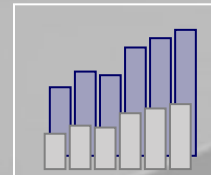
- Доступен начиная с 10.2В
- Отдельный продукт
- Лицензируется отдельно
- Необходима Enterprise лицензия



# Как работает TDE?

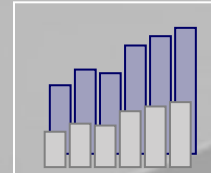


# Как работает TDE?



- Key Store
  - Database Master Key
  - Admin/User Passphrase
  - Manual/Automatic Authentication
- Encryption Policy Area
  - Encryption Policy – Что (объект) и Как (Шифр)

# The Key Store



## Уникальное название

- Имя файла: <dbname.ks>

## Содержит Database Master Key (DMK)

- Обеспечивает уникальность зашифрованных данных

## Обеспечивает безопасность DMK

- Хранилище отделено от базы данных
- Защита доступа к хранилищу на основе Passphrase
- Не входит в состав резервной копии (PROBKUP)

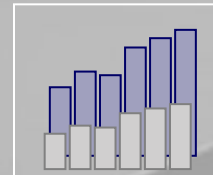
Your database backup is not complete until you have made an OS backup or copy of your keystore.  
(15525)

## Почему?



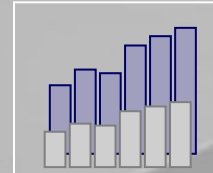


# Правила формирования Passphrase



- Количество символов: от 8 до 2048
- Набор символов: [a-zA-Z0-9]!@#\$%^&\*()\_+~{}[]\|,./<>?:;<space>
- Минимальное количество целочисленных символов: 1
- Минимальное количество буквенных символов: 2
- Минимальное количество символов пунктуации: 1
- Максимальное количество повторяющихся символов: 0
- Использование верхнего и нижнего регистра: Да
- Чувствительность к регистру: Да

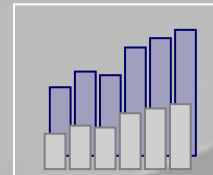




ID	Шифр	Режим	Длина	Тип ключа
1	AES	CBC	128	BINARY
2	AES	CBC	192	BINARY
3	AES	CBC	256	BINARY
4	DES	CBC	56	BINARY
5	DES3	CBC	168	BINARY
6	DES	CBC	56	PBE
7	RC4	ECB	128	BINARY



# The Encryption Policy



## Содержимое политики шифрования

- Объекты шифрования
  - ✓ Таблица, Индекс, LOB (SAT-II)
  - ✓ Область хранения (SAT-I)
  - ✓ AI/BI
- Шифр
  - ✓ Алгоритм
  - ✓ Длина ключа

## Безопасность

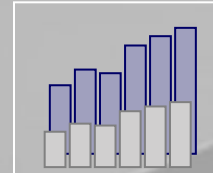
- Отдельная область хранения (Encryption Policy Area)
- Защита от прямого доступа

## Обслуживание

- EPOLICY MANAGE, Data Admin, OpenEdge SQL DDL
- Добавление, удаление, изменение ключа или шифра в online



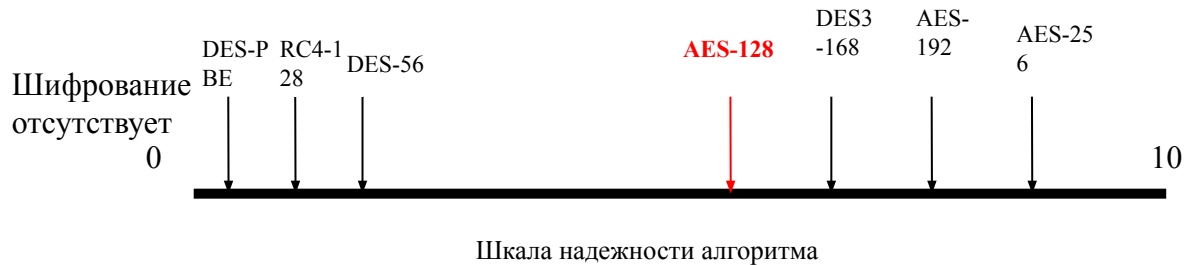
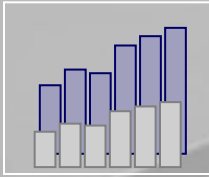
# Шифры политик шифрования



ID	Шифр	Режим	Длина	Тип ключа
0	NULL	NULL	-	-
1	AES	CBC	128	BINARY
2	AES	CBC	192	BINARY
3	AES	CBC	256	BINARY
4	DES	CBC	56	BINARY
5	DES3	CBC	168	BINARY
7	RC4	ECB	128	BINARY



# Выбор шифра

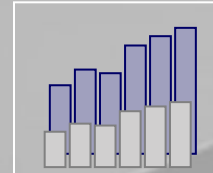


Политика безопасности

Баланс между надежностью и производительностью



# Шаг №1: Включение шифрования.



1. Создайте новую область хранения SAT-II  
е “**Encryption Policy Area**”:12,**32;64** . f 1024  
е .
2. С помощью PROSTRC ADD/ADDONLINE добавьте область в базу

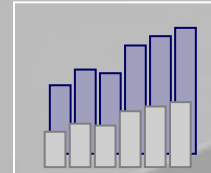
```
prostrct add mydb encrypt.st
```

3. Обновите структурный файл базы данных

```
prostrct list mydb
```



## Шаг №2: Включение шифрования.



**proutil <dbname> -C enableencryption**

**[-Cipher <cipher-num>]**

**[-Autostart]**

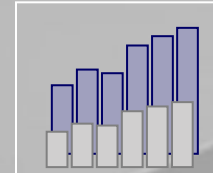
**[-biencryption enable | disable]**

**[-aiencryption enable | disable]**

- Будет усечен VI файл (offline)
- Будет создано хранилище ключей <dbname>.ks
- В область Encryption Policy Area будет загружена схема
- Будет запрошен Passphrase (User/Admin)
- Сгенерирован DMK
- Сгенерированы ключи для AI и VI, если не указано обратное
- Настроен Autostart
  - Manual/Automatic
- Появится возможность создания политик шифрования
  
- Шифрование данных не происходит!



# Включение шифрования. Шаг №3.



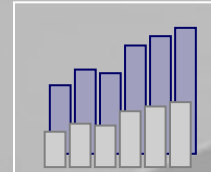
## Способы создания политик шифрования

- ❑ EPOLICY MANAGE
- ❑ Data Admin
- ❑ OpenEdge SQL DDL





# Шаг №3: Epolicy Manage



```
proutil <dbname> -C epolicy manage <object-type>  
    encrypt | cipher | rekey <object-name>  
-Cipher < num >
```

```
$ proutil sports -C epolicy manage area encrypt "TestArea1"
```

```
Encryption policy setting for Area TestArea1 in Area 7 (15504)  
Cipher specification setting to AES_CBC_128 completed. (15491)
```

```
$ proutil sports -C epolicy scan area "TestArea1"
```

```
OpenEdge Release 10.2B1B as of Thu Jul 30 19:00:21 EDT 2009  
AREA TestArea1 / 7 CURRENT AES_CBC_128 V:0 79 of 1784 blocks encrypted
```

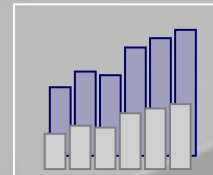
```
$ proutil sports -C epolicy manage area update "TestArea1"
```

```
OpenEdge Release 10.2B1B as of Thu Jul 30 19:00:21 EDT 2009  
AREA TestArea1 / 7 CURRENT AES_CBC_128 V:0 1705 of 1784 blocks encrypted
```

- Шифрование области (**object-type = Area**) доступно только для **SAT-I**
- Объекты **Table, Index, LOB** должны размещаться в области **SAT-II**
- Данные могут быть зашифрованы тремя способами:
  - Естественный процесс шифрования
  - Dump & Load
  - PROUTIL EPOLICY MANAGE UPDATE



# Шаг №3: Data Admin



## Меню: Admin -> Security -> Encryption Policies -> Edit Encryption Policy

**Object Selector**  
Select one or more objects with the [SPACEBAR] key.  
Press [F1] to go to the next screen.

<Select Some...>                      <Deselect Some...>

adr-a.datazm	Idx
adr-a.rachunek	Idx
adr-a.rachunek	Idx

**Edit Encryption Policy**  
Objects (\* = changed policy):

>adr-a.datazm  
adr-a.rachunek

**Copy Encryption Policy Settings To**  
If you want to copy the settings from the encryption policy of the current object to other object(s), select them on the list below.

<Select Some...>                      <Deselect Some...>

adr-a.rachunek	Idx
----------------	-----

**Review Changes**

Summary of changes to encryption policies  
-----  
Enable encryption with cipher 'AES\_CBC\_128' for objects:  
adr-a.datazm (Index)  
adr-a.rachunek (Index)

**Question**  
You are about to save the changes to the database.  
Do you want to proceed ?

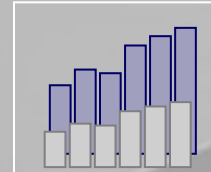
<Yes>    <No>

<Close>

- Только для SAT-II
- Только для PUB схемы
- Для более чем одного объекта
- Только локальный доступ
- Шифрование:
  - Естественное
  - D&L
  - EPOLICY UPDATE



# Шаг №3: OpenEdge SQL DDL



```
CREATE TABLE PUB.enctab1  
(encid int, encdes int, encdt varchar(25))  
AREA "TestArea2"  
ENCRYPT WITH 'AES_CBC_192';  
COMMIT;
```

```
CREATE INDEX idx1  
ON PUB.ENCTAB1  
(encid ASC)  
AREA "TestArea2"  
ENCRYPT WITH 'AES_CBC_192';  
COMMIT;
```

```
ALTER TABLE PUB.ENCTAB1  
SET ENCRYPT WITH 'AES_CBC_128';  
COMMIT;
```

```
ALTER TABLE PUB.ENCTAB1  
SET ENCRYPT REKEY;  
COMMIT;
```

```
ALTER TABLE PUB.ENCTAB1  
SET DECRYPT;  
COMMIT;
```

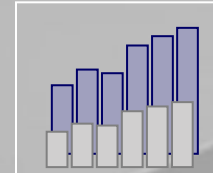
```
$ proutil sports -C epolicy manage table update ENCTAB1
```

```
SHOW ENCRYPT ON ALL | TABLE | INDEX | LOB |;
```

OBJECT TYPE	OBJECT NAME	OBJECT TABLE	OBJECT OWNER	OBJECT ID	OBJECT POLICY STATE	OBJECT POLICY CIPHERSPEC	POLICY VERSION
TABLE	ENCTAB1	ENCTAB1	PUB	855	CURRENT	AES_CBC_192	0
INDEX	IDX1	ENCTAB1	PUB	2428	CURRENT	AES_CBC_192	0
AREA	TestArea1			7	CURRENT	AES_CBC_128	0



# Шаг №3: Data Definition File (.df)



## □ UPDATE TABLE

□ **ENCRYPTION YES**

□ **CIPHER-NAME** <полное название шифра>

## □ DEFINITION TRAILER

□ **encpolicy=yes**

```
ADD TABLE "ENCTAB1"  
  AREA "TestArea2"  
  DUMP-NAME "ENCTAB1"
```

```
ADD FIELD "ENCID" OF "ENCTAB1" AS integer  
  FORMAT "->,>>>,>>9"  
  INITIAL "?"  
  POSITION 2  
  MAX-WIDTH 4  
  ORDER 10
```

```
ADD FIELD "ENCDT" OF "ENCTAB1" AS character  
  FORMAT "x(8)"  
  INITIAL "?"  
  POSITION 4  
  MAX-WIDTH 25  
  LENGTH 0  
  ORDER 30  
  CASE-SENSITIVE
```

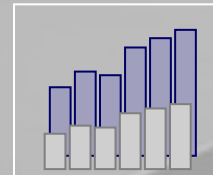
```
ADD INDEX "IDX1" ON "ENCTAB1"  
  AREA "TestArea2"  
  PRIMARY  
  INDEX-FIELD "ENCID" ASCENDING
```

```
UPDATE TABLE "ENCTAB1"  
  ENCRYPTION YES  
  CIPHER-NAME AES_CBC_192
```

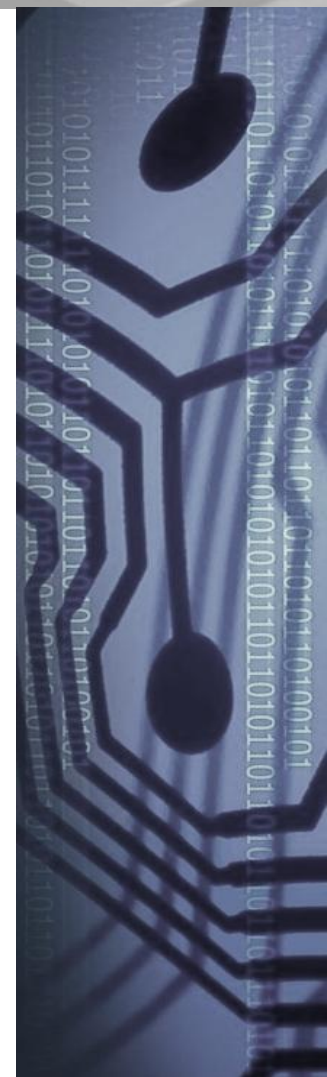
```
.  
PSC  
encpolicy=yes  
cpstream=ibm866  
.  
000000605
```



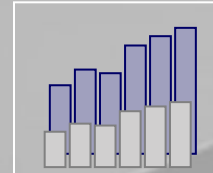
# TDE и OpenEdge Replication



- TDE для Source и Target базы данных должен быть включен
- Шифрование VI для Target только после пересоздания Target
- Шифрование AI для Target включается автоматически Агентом репликации
- Номера областей Encryption Policy Area должны быть одинаковыми
- Хранилище ключей (*dbname.ks*), копируется с Source базы данных

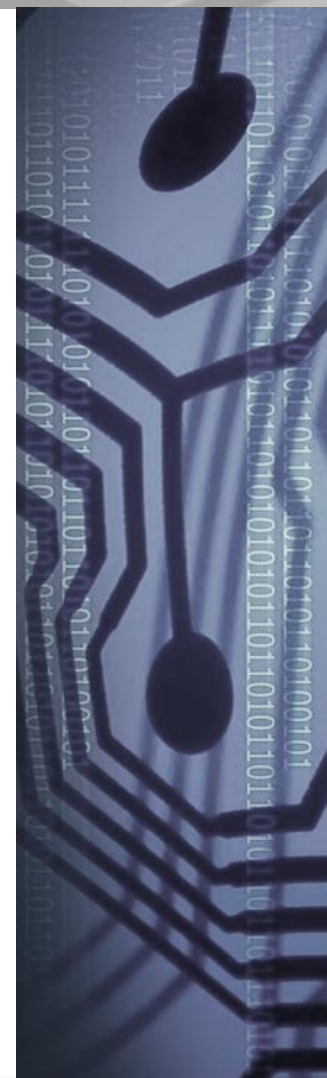


# TDE и OpenEdge Replication

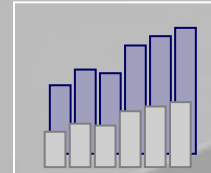


TDE для базы с OE Replication offline / **online**

1. **Остановить Target базу данных**
2. Добавить область Encryption Policy Area в Source и Target базы
3. Включить шифрование на Source базе
4. Настроить политики шифрования на Source базе
5. **Скопировать хранилище ключей (dbname.ks) с Source на Target**
6. Старт:
  - Source и Target базы данных.
  - **Target**



# Выключение TDE



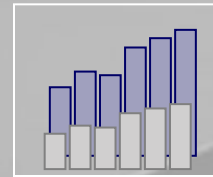
```
proutil <dbname> -C epolicy manage object-type cipher object-name -Cipher 0  
proutil <dbname> -C epolicy manage object-type update object-name
```

```
proutil <dbname> -C disableencryption  
  [-Passphrase]  
  [  
    [-userid userid]  
    [-password password]  
  ]
```

- Отключается шифрование BI (только в offline)
- Отключается шифрование AI
- Все данные расшифровываются
- Удаляются все политики шифрования
- Архивируется хранилище ключей, файл .ks переименовывается в .ksbk.



# Производительность



## 1. Показания Buffer Hit Rate

- ❑ Увеличьте Буферный пул (-B)
- ❑ Используйте Альтернативный буферный пул для зашифрованных объектов (-B2)

## 2. Нормализация данных

- ❑ Отделите конфиденциальную информацию от обычной
- ❑ Используйте область с типом SAT-II
- ❑ Тщательно выбирайте индексы для шифрования

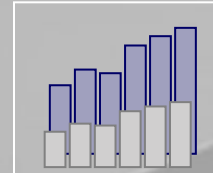
## 3. Тщательно выбирайте шифр (алгоритм + длина ключа)

- ❑ Баланс между безопасностью и производительностью





**ВНИМАНИЕ!**



**управляя информацией**

**OpenEdge 10.2B: Transparent Data Encryption**

Башкатов Валерий Григорьевич

[v.bashkatov@csbi.ru](mailto:v.bashkatov@csbi.ru)

[www.openedge.ru](http://www.openedge.ru)

