Средства защиты от НСД в ОС семейства Windows

Синадский Н.И. 1998-2018

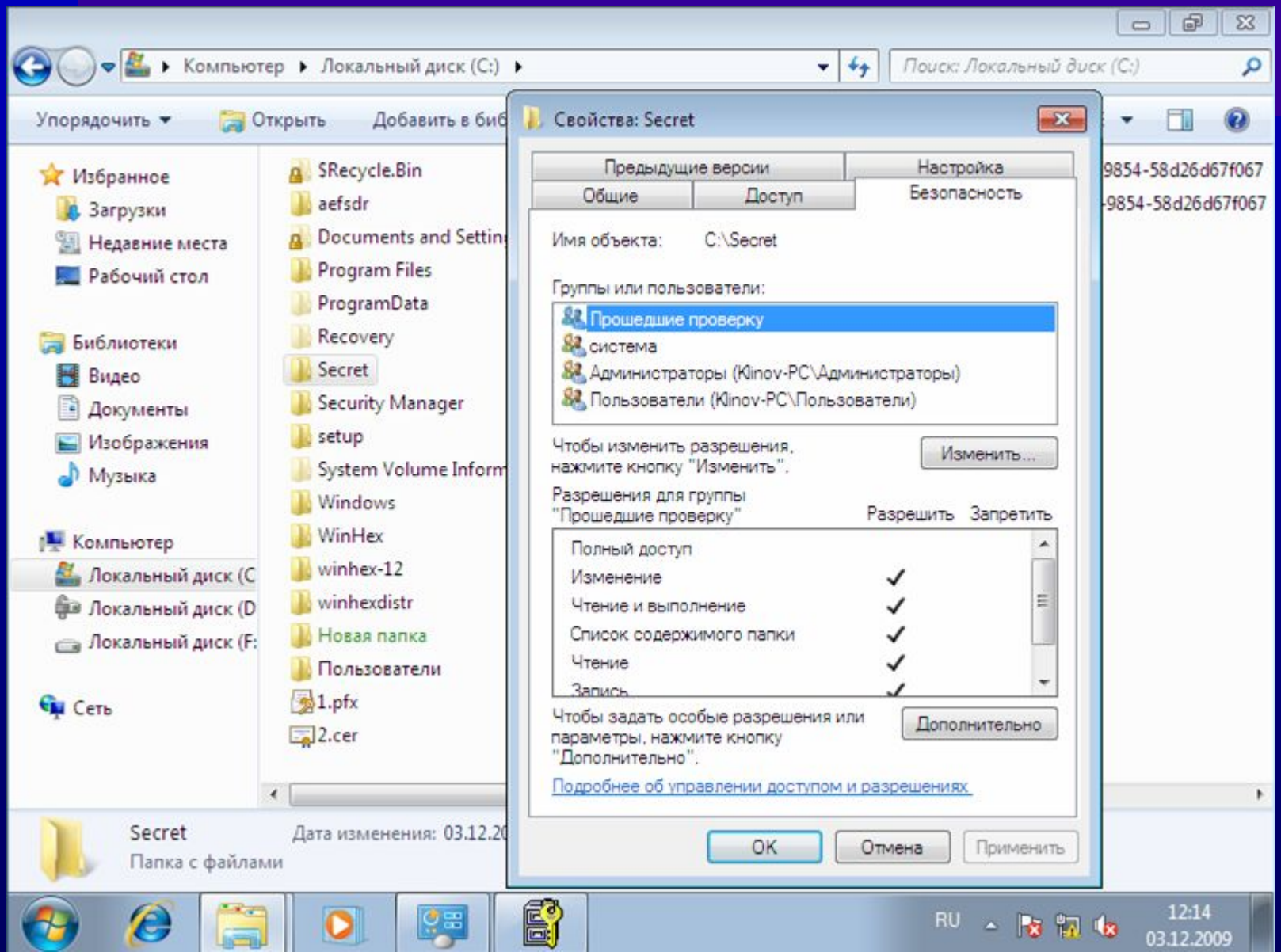
Учебные вопросы

- Разграничение доступа средствами NTFS
- Аудит событий безопасности
- Шифрующая ФС
- Хранение парольной информации
- Структура файлов реестра
- Шифрование парольной информации
- Атаки на пароли
- BitLocker drive encryption

Семейство ОС Windows NT – 2000 – XP – 7

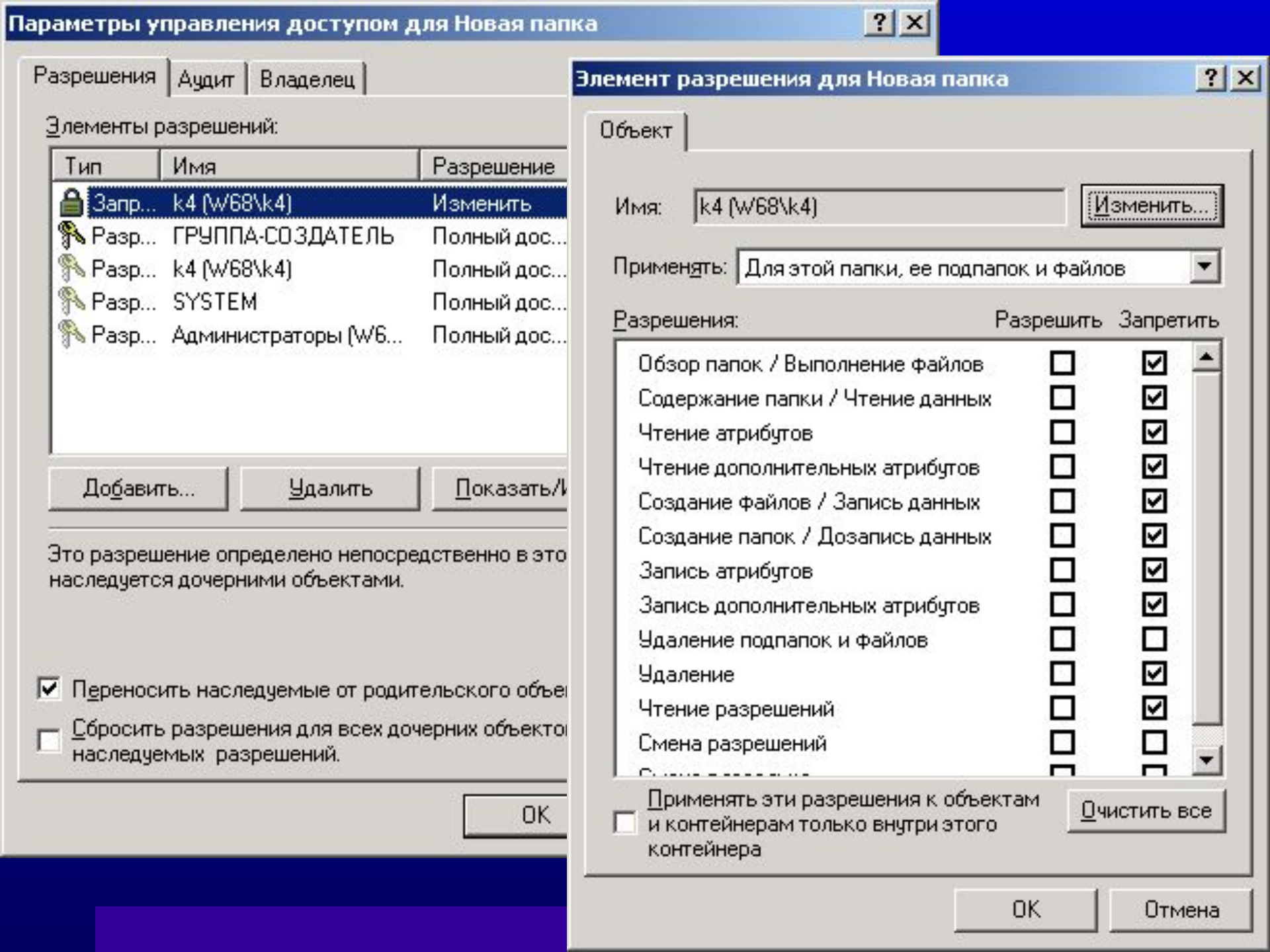
- Windows NT 3.51
- Windows NT 4.0 Workstation, Server
- Windows 2000 Professional, Server, Advanced Server, …
- Windows XP, 2003 Server
- Windows Vista
- Windows 7, 8, 10, Server 2008, Server 2012

Списки доступа



- Список доступа (VAX/VMS, Windows NT)
  - С каждым объектом ассоциируется список переменной длины, элементы содержат:
    - идентификатор субъекта
    - права, предоставленные этому субъекту на данный объект
  - Access Control List

	Файл 1
User 1	R
User 2	R
User 3	RW


Параметры управления доступом для Новая папка
Разрешения
Аудит
Владелец
Элементы разрешений:
Тип
Имя
Разрешение
Запр... k4 (W68\k4) Изменить
Разр... ГРУППА-СОЗДАТЕЛЬ Полный дос...
Разр... k4 (W68\k4) Полный дос...
Разр... SYSTEM Полный дос...
Разр... Администраторы (W6... Полный дос...
Добавить...
Удалить
Показать/
Это разрешение определено непосредственно в это
наследуется дочерними объектами.
Переносить наследуемые от родительского объе
Сбросить разрешения для всех дочерних объекто
наследуемых разрешений.
OK
Элемент разрешения для Новая папка
Объект
Имя: k4 (W68\k4)
Изменить...
Применять: Для этой папки, ее подпапок и файлов
Разрешения:
Разрешить
Запретить
Обзор папок / Выполнение файлов
Содержание папки / Чтение данных
Чтение атрибутов
Чтение дополнительных атрибутов
Создание файлов / Запись данных
Создание папок / Дозапись данных
Запись атрибутов
Запись дополнительных атрибутов
Удаление подпапок и файлов
Удаление
Чтение разрешений
Смена разрешений
Применять эти разрешения к объектам
и контейнерам только внутри этого
контейнера
Очистить все
OK
Отмена

Информация о правах доступа (разрешениях)

- Где хранить списки доступа?
  - В отдельном общем файле ?
  - Внутри каждого файла ?
- Файловая система должна поддерживать списки доступа
- Файловая система NTFS в ОС Windows NT -2000

- Небольшой файл в NTFS

DOS - атрибуты, время, ...

До 255 UNICODE

Список прав доступа Access Control List (ACL)

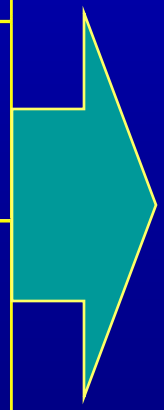
Как формировать ACL?

Идентификация пользователей

- У любого пользователя:
  - имя пользователя
  - уникальный идентификатор
- Идентификатор безопасности – SID
  - (Security ID)

ACL файла «Файл 1»

	Файл 1
User 1	R
User 2	R
User 3	RW



ACL

12278633-1016	R
12278633-1017	R
12278633-1018	RW

Дескриптор защиты

- Структура данных, описывающая объект:
  - SID владельца объекта
  - Дискреционный список контроля доступа (DACL)
  - Системный список контроля доступа (SACL)

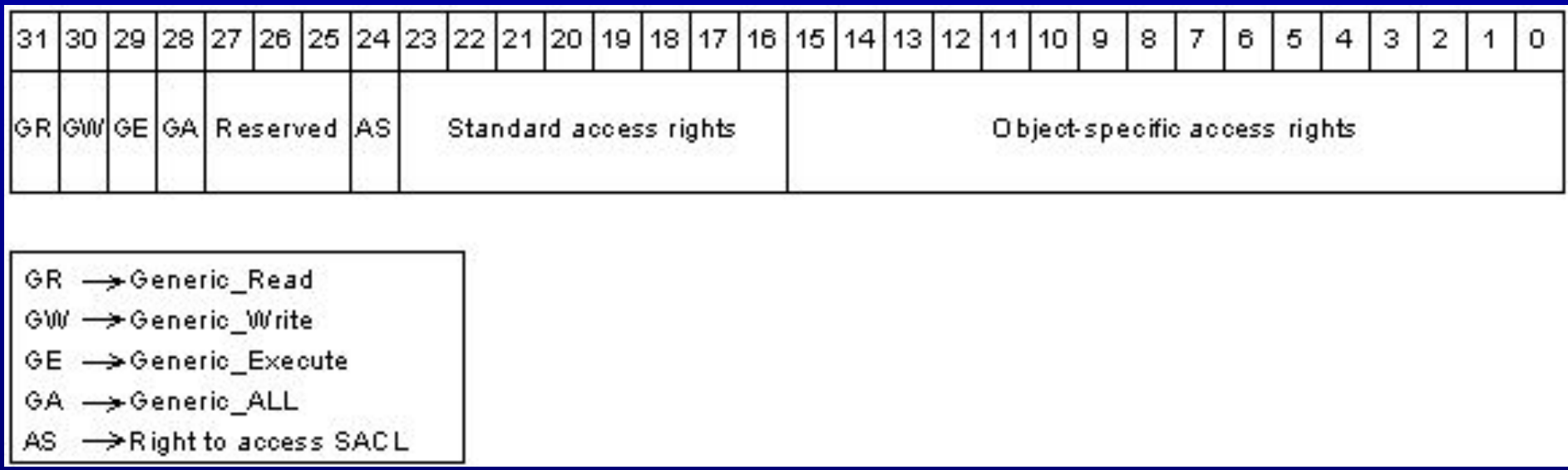
Дискреционный список контроля доступа (DACL)

- Discretionary Access Control List (DACL) - список, в котором перечислены права пользователей и групп на доступ к объекту
- Обычно устанавливает владелец объекта
- Каждый элемент списка - запись контроля доступа (Access Control Entry, ACE), которая указывает права конкретной учетной записи

Записи контроля доступа (ACE)

- Три типа записей:
  - «доступ запрещен» - отклоняет доступ к объекту для данного пользователя
  - «доступ разрешен»
  - «системный аудит»
- Каждая запись содержит (в частности):
  - маску, определяющую набор прав на доступ к объекту и
  - идентификатор безопасности, к которой применяется маска

Маска доступа – Access Mask

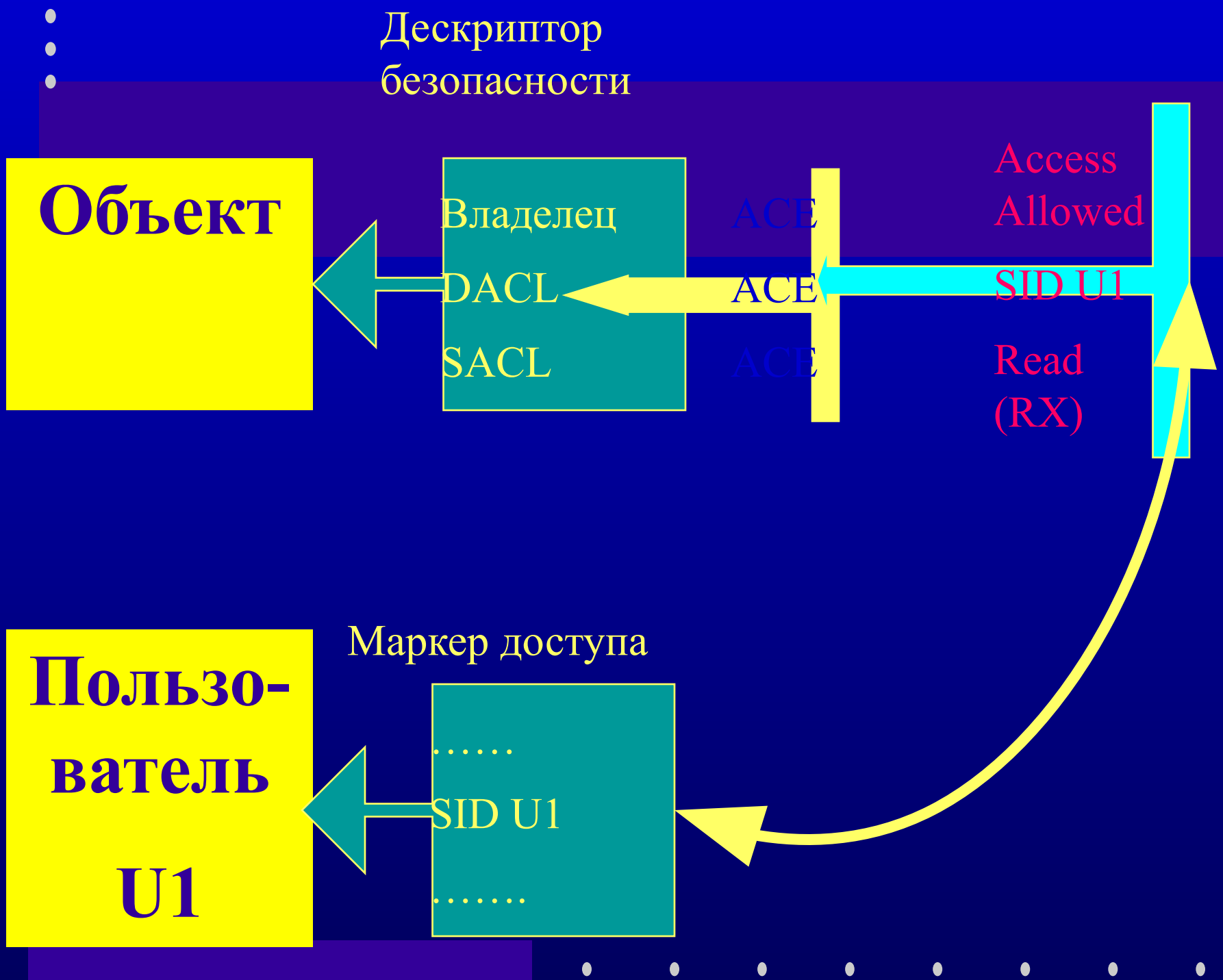


Маркер доступа

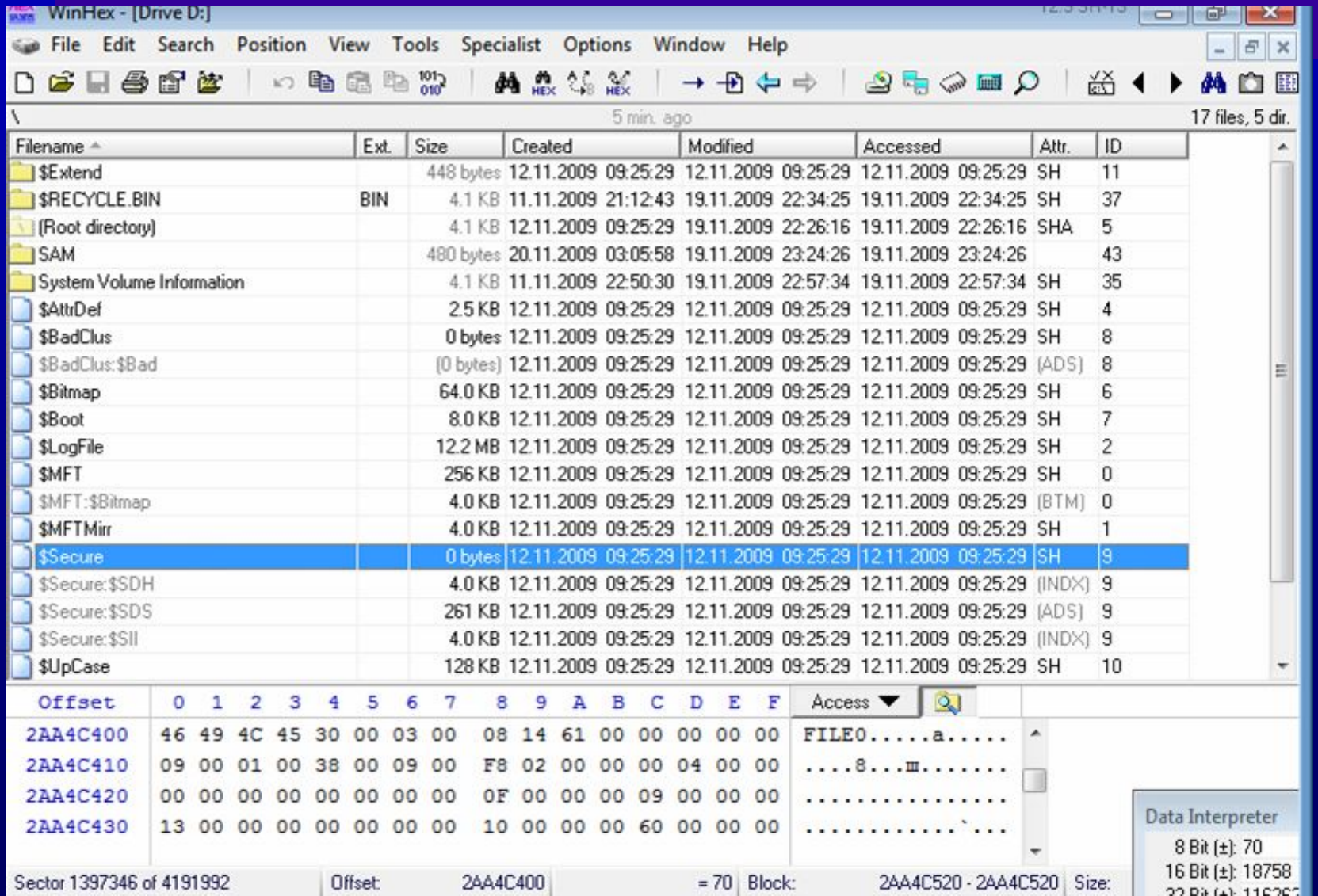
- Маркер доступа (access token) - структура данных, содержащая
  - SID пользователя
  - Массив SID групп, к которым принадлежит пользователь
  - Массив прав пользователя

Контроль доступа

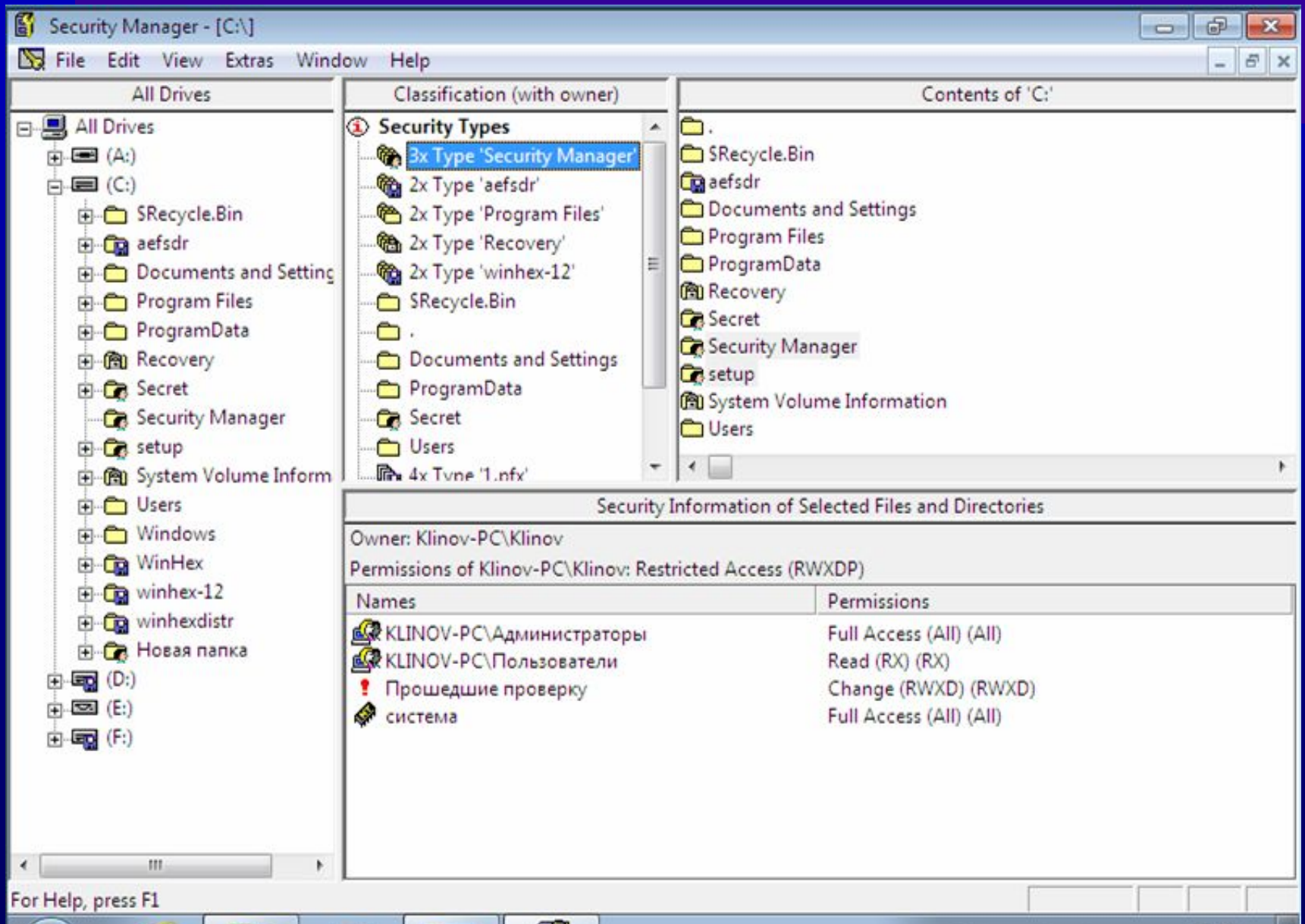
- Осуществляется монитором безопасности
- Сравнение информации безопасности в маркере доступа пользователя с информацией в дескрипторе безопасности объекта
- Происходит последовательное сравнение SID всех записей ACE со всеми SID пользователя из маркера доступа


Дескриптор безопасности
Объект
Владелец
DACL
SACL
ACE
ACE
ACE
Access Allowed
SID U1
Read (RX)
Маркер доступа
.....
SID U1
.....
Пользо-ватель U1

Файл $Secure


WinHex - [Drive D:]
File Edit Search Position View Tools Specialist Options Window Help
\ 5 min. ago 17 files, 5 dir.
Filename Ext. Size Created Modified Accessed Attr. ID
$Extend 448 bytes 12.11.2009 09:25:29 12.11.2009 09:25:29 12.11.2009 09:25:29 SH 11
$RECYCLE.BIN BIN 4.1 KB 11.11.2009 21:12:43 19.11.2009 22:34:25 19.11.2009 22:34:25 SH 37
(Root directory) 4.1 KB 12.11.2009 09:25:29 19.11.2009 22:26:16 19.11.2009 22:26:16 SHA 5
SAM 480 bytes 20.11.2009 03:05:58 19.11.2009 23:24:26 19.11.2009 23:24:26 43
System Volume Information 4.1 KB 11.11.2009 22:50:30 19.11.2009 22:57:34 19.11.2009 22:57:34 SH 35
$AttrDef 2.5 KB 12.11.2009 09:25:29 12.11.2009 09:25:29 12.11.2009 09:25:29 SH 4
$BadClus 0 bytes 12.11.2009 09:25:29 12.11.2009 09:25:29 12.11.2009 09:25:29 SH 8
$BadClus:$Bad (0 bytes) 12.11.2009 09:25:29 12.11.2009 09:25:29 12.11.2009 09:25:29 (ADS) 8
$Bitmap 64.0 KB 12.11.2009 09:25:29 12.11.2009 09:25:29 12.11.2009 09:25:29 SH 6
$Boot 8.0 KB 12.11.2009 09:25:29 12.11.2009 09:25:29 12.11.2009 09:25:29 SH 7
$LogFile 12.2 MB 12.11.2009 09:25:29 12.11.2009 09:25:29 12.11.2009 09:25:29 SH 2
$MFT 256 KB 12.11.2009 09:25:29 12.11.2009 09:25:29 12.11.2009 09:25:29 SH 0
$MFT:$Bitmap 4.0 KB 12.11.2009 09:25:29 12.11.2009 09:25:29 12.11.2009 09:25:29 (BTM) 0
$MFTMirr 4.0 KB 12.11.2009 09:25:29 12.11.2009 09:25:29 12.11.2009 09:25:29 SH 1
$Secure 0 bytes 12.11.2009 09:25:29 12.11.2009 09:25:29 12.11.2009 09:25:29 SH 9
$Secure:$SDH 4.0 KB 12.11.2009 09:25:29 12.11.2009 09:25:29 12.11.2009 09:25:29 (INDX) 9
$Secure:$SDS 261 KB 12.11.2009 09:25:29 12.11.2009 09:25:29 12.11.2009 09:25:29 (ADS) 9
$Secure:$SII 4.0 KB 12.11.2009 09:25:29 12.11.2009 09:25:29 12.11.2009 09:25:29 (INDX) 9
$UpCase 128 KB 12.11.2009 09:25:29 12.11.2009 09:25:29 12.11.2009 09:25:29 SH 10
Offset 0 1 2 3 4 5 6 7 8 9 A B C D E F Access
2AA4C400 46 49 4C 45 30 00 03 00 08 14 61 00 00 00 00 00 FILE0.....a.....
2AA4C410 09 00 01 00 38 00 09 00 F8 02 00 00 00 04 00 00 ....8...m.....
2AA4C420 00 00 00 00 00 00 00 00 0F 00 00 00 09 00 00 00 ....
2AA4C430 13 00 00 00 00 00 00 00 10 00 00 00 60 00 00 00 ....`...
Data Interpreter
8 Bit (±): 70
16 Bit (±): 18758
Sector 1397346 of 4191992 Offset: 2AA4C400 = 70 Block: 2AA4C520 - 2AA4C520 Size:

Программа Security Manager



Реестр ОС

- Ветвь реестра Файл
- HKEY_LOCAL_MACHINE\SYSTEM system
- HKEY_LOCAL_MACHINE\SAM sam
- HKEY_LOCAL_MACHINE\SECURITY security
- HKEY_LOCAL_MACHINE\SOFTWARE software
- HKEY_LOCAL_MACHINE\ HARDWARE Временная ветвь
- HKEY_USERS\.DEFAULT default
- HKEY_CURRENT_USER NTUSER.DAT

РЕГИСТРАЦИЯ СОБЫТИЙ БЕЗОПАСНОСТИ

Аудит

Событие безопасности (информационной): идентифицированное возникновение состояния ИС, сервиса или сети, указывающее на

- возможное нарушение безопасности информации,
- или сбой средств защиты информации,
- или ранее неизвестную ситуацию, которая может быть значимой для безопасности информации

Хранение - не менее трех месяцев

РСБ Определение событий безопасности

- вход (выход), а также попытки входа субъектов доступа в ИС и загрузки (останова) ОС;
- подключение МНИ и вывод информации на МНИ;
- запуск (завершение) программ и процессов (заданий, задач), связанных с обработкой защищаемой информации;
- попытки доступа программных средств к защищаемым объектам доступа;
- попытки удаленного доступа
- действия от имени привилегированных учетных записей (администраторов)
- изменение привилегий учетных записей

Состав и содержание информации о событиях безопасности

- тип
- дата и время
- источник
- результат (успешно или неуспешно)
- субъект доступа (пользователь и (или) процесс)

- Доступ к записям аудита и функциям управления - только уполномоченным должностным лицам

Аудит событий безопасности

- Аудит - регистрация в журнале событий, которые могут представлять опасность для ОС
- Аудитор ? Администратор

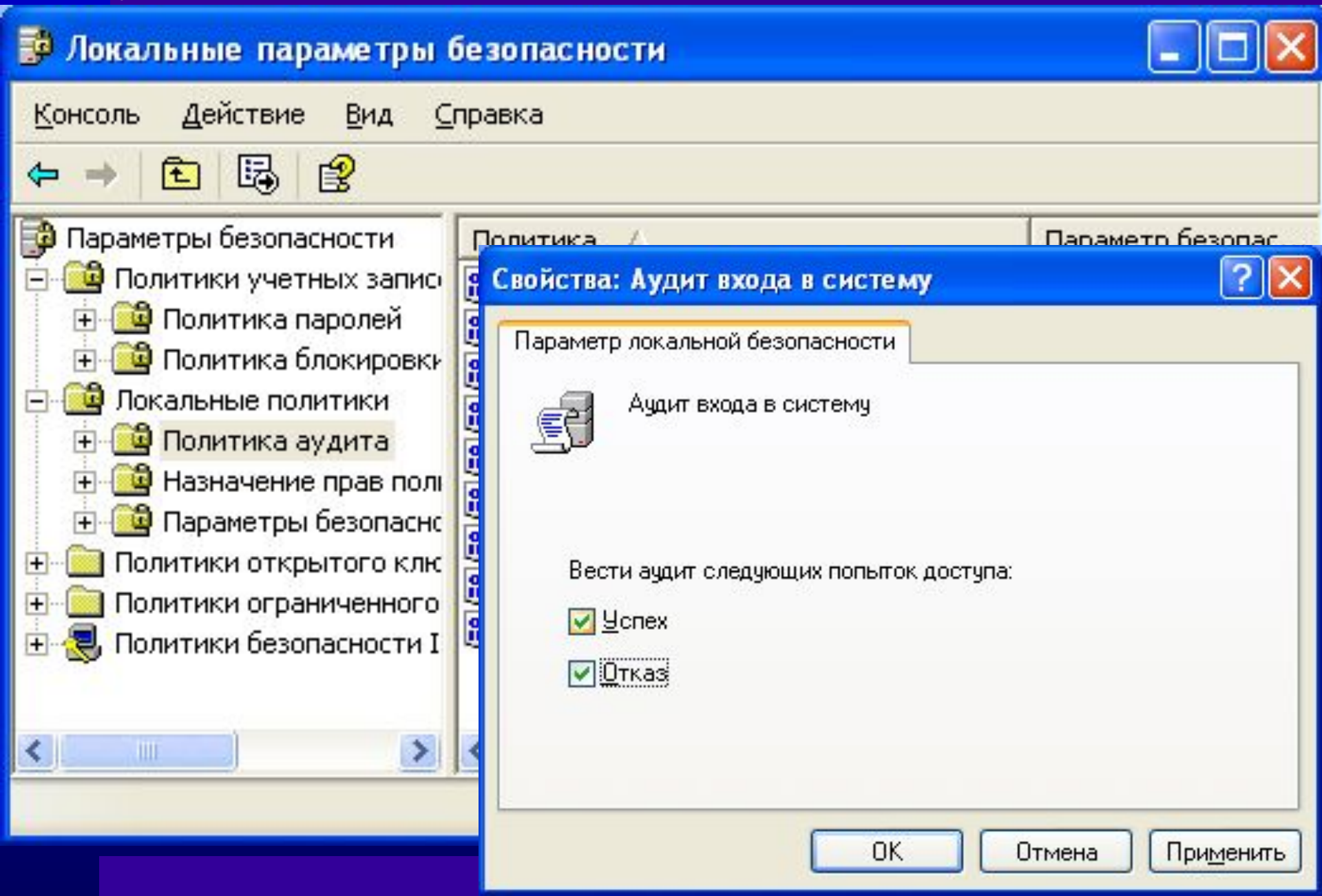
Требования к аудиту

- Только сама ОС может добавлять записи в журнал
- Ни один субъект доступа, в т.ч. ОС, не имеет возможности редактировать отдельные записи
- Только аудиторы могут просматривать журнал
- Только аудиторы могут очищать журнал
- При переполнении журнала ОС аварийно завершает работу

Журнал - это файл => может быть получен доступ в обход ОС

Политика аудита

- Совокупность правил, определяющая то, какие события должны регистрироваться:
  - вход/выход пользователей из системы
  - изменение списка пользователей
  - изменения в политике безопасности
  - доступ субъектов к объектам
  - использование опасных привилегий
  - системные события
  - запуск и завершение процессов


Локальные параметры безопасности
Консоль
Действие
Вид
Справка
Параметры безопасности
Политики учетных запис
Политика паролей
Политика блокировки
Локальные политики
Политика аудита
Назначение прав поли
Параметры безопасно
Политики открытого клю
Политики ограниченного
Политики безопасности I
Политика
Параметр безопас
Свойства: Аудит входа в систему
Параметр локальной безопасности
Аудит входа в систему
Вести аудит следующих попыток доступа:
Успех
Отказ
OK
Отмена
Применить

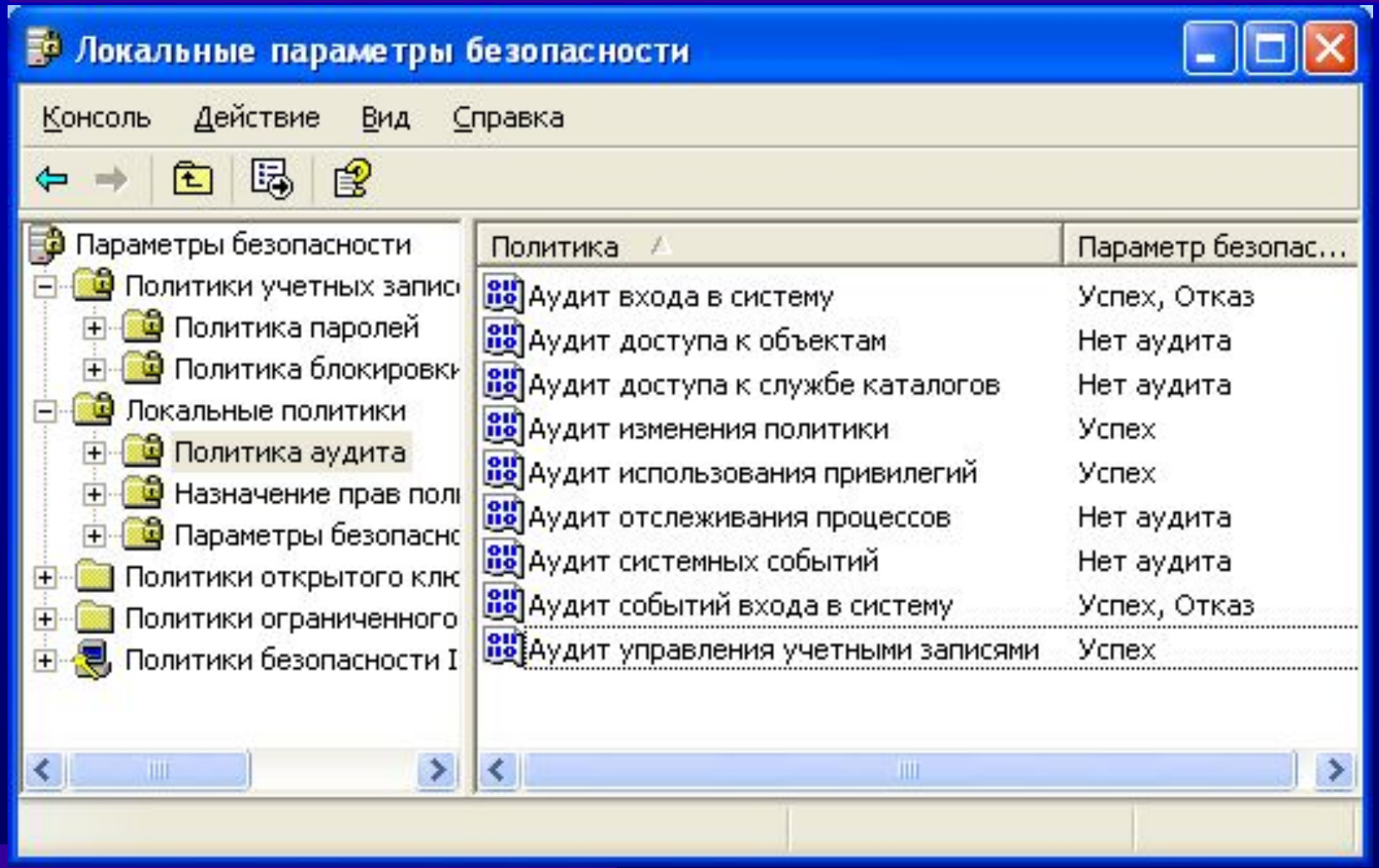
Адекватная политика аудита

- Регистрируется ровно столько событий, сколько необходимо
- Рекомендации
  - вход и выход пользователей регистрируются всегда
  - доступ субъектов к объектам регистрировать только в случае обоснованных подозрений злоупотребления полномочиями

Адекватная политика аудита

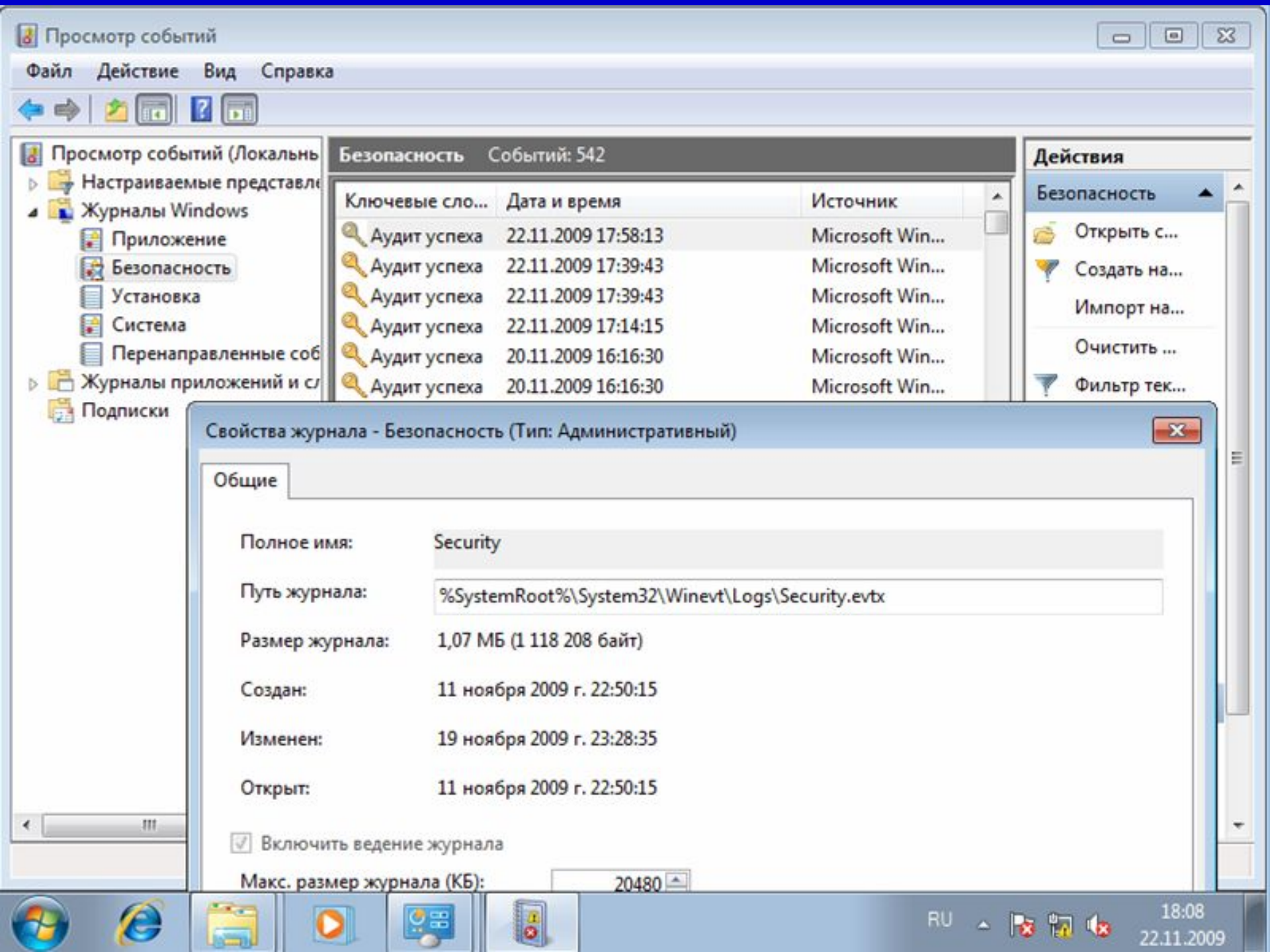
- регистрировать применение опасных привилегий
- регистрировать только успешные попытки внесения изменений в список пользователей
- регистрировать изменения в политике безопасности
- не регистрировать системные события
- не регистрировать запуск и завершение процессов, кроме случая обоснованных подозрений вирусных атак

Адекватная политика аудита



Журналы аудита

- SecEvent.Evt, SysEvent.Evt и AppEvent.Evt
- %SystemRoot%\System32\
  - config
  - Winevt\logs
- Путь к файлам журнала в реестре
  - HKLM\SYSTEM\CurrentControlSet\Services\EventLog


Просмотр событий
Файл Действие Вид Справка
Просмотр событий (Локальнь
Настраиваемые представле
Журналы Windows
Приложение
Безопасность
Установка
Система
Перенаправленные соб
Журналы приложений и сл
Подписки
Безопасность Событий: 542
Ключевые сло... Дата и время Источник
Аудит успеха 22.11.2009 17:58:13 Microsoft Win...
Аудит успеха 22.11.2009 17:39:43 Microsoft Win...
Аудит успеха 22.11.2009 17:39:43 Microsoft Win...
Аудит успеха 22.11.2009 17:14:15 Microsoft Win...
Аудит успеха 20.11.2009 16:16:30 Microsoft Win...
Аудит успеха 20.11.2009 16:16:30 Microsoft Win...
Действия
Безопасность
Открыть с...
Создать на...
Импорт на...
Очистить ...
Фильтр тек...
Свойства журнала - Безопасность (Тип: Административный)
Общие
Полное имя: Security
Путь журнала: %SystemRoot%\System32\Winevt\Logs\Security.evtx
Размер журнала: 1,07 МБ (1 118 208 байт)
Создан: 11 ноября 2009 г. 22:50:15
Изменен: 19 ноября 2009 г. 23:28:35
Открыт: 11 ноября 2009 г. 22:50:15
Включить ведение журнала
Макс. размер журнала (КБ): 20480
RU
18:08
22.11.2009

Важнейшие коды событий

- 512 Запуск Windows NT
- 513 Завершение работы Windows NT
- 517 Журнал аудита очищен
- 528 Успешная регистрация
- 529 Неудачная регистрация (неизвестное имя пользователя или неверный пароль)
- 560 Объект открыт

Идентификация пользователей

- по имени учетной записи пользователя
- учетная запись ⇔ SID

SID S-1-5-21-2113235361-147094754-1228766249-500

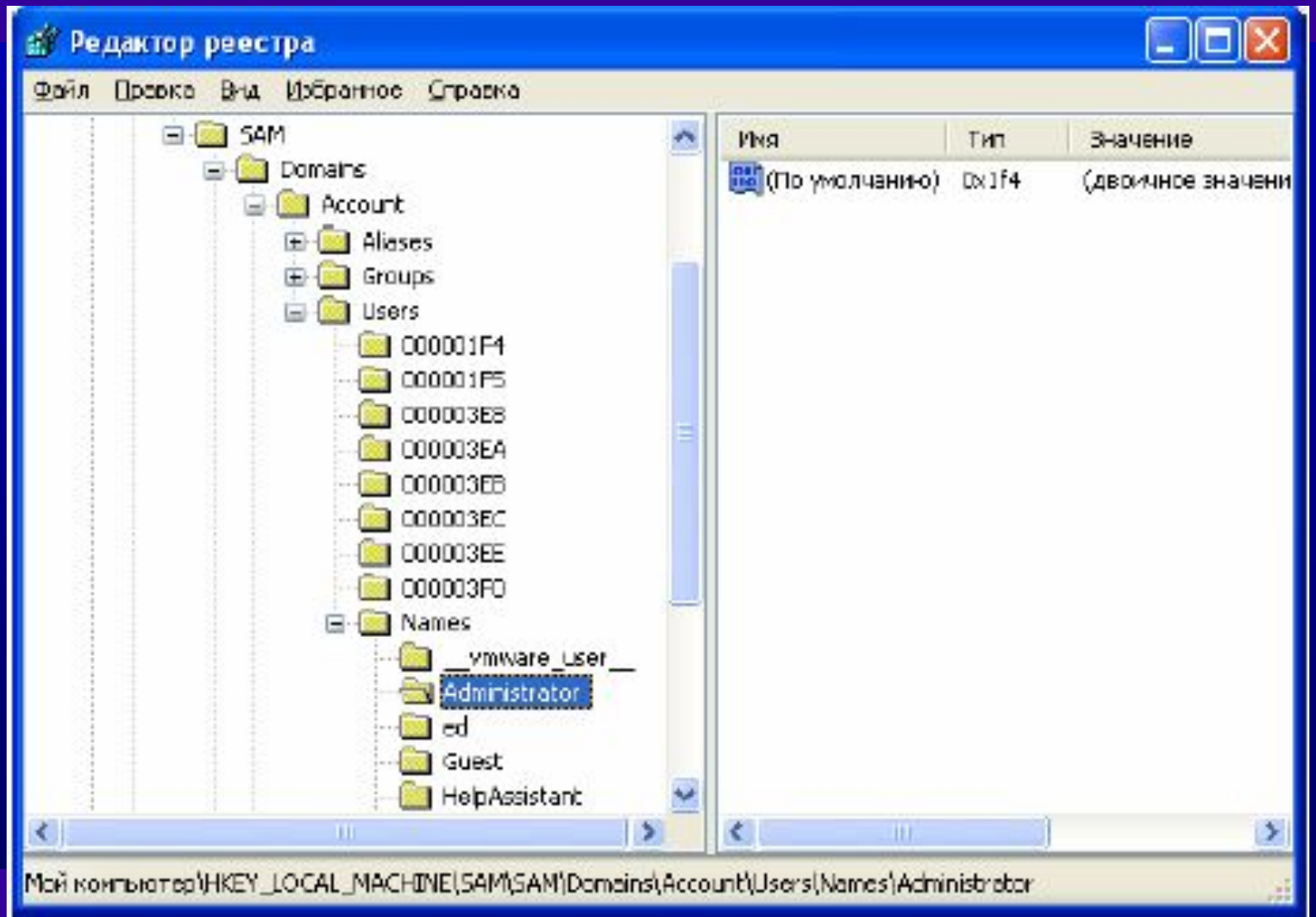
SID S-1-5-21-2113235361-147094754-1228766249-500

S-1-5-21-2113235361-147094754-1228766249-501

S-1-5-21-2113235361-147094754-1228766249-512

- Относительные идентификаторы (RID) - идентификаторы безопасности с предопределенным последним номером подразделения (для встроенных учетных записей)
- Например:
  - 500 - admninstrator
  - 501 - Guest
  - 512 - Domain Admins

Учетные записи в файле SAM



Параметр F

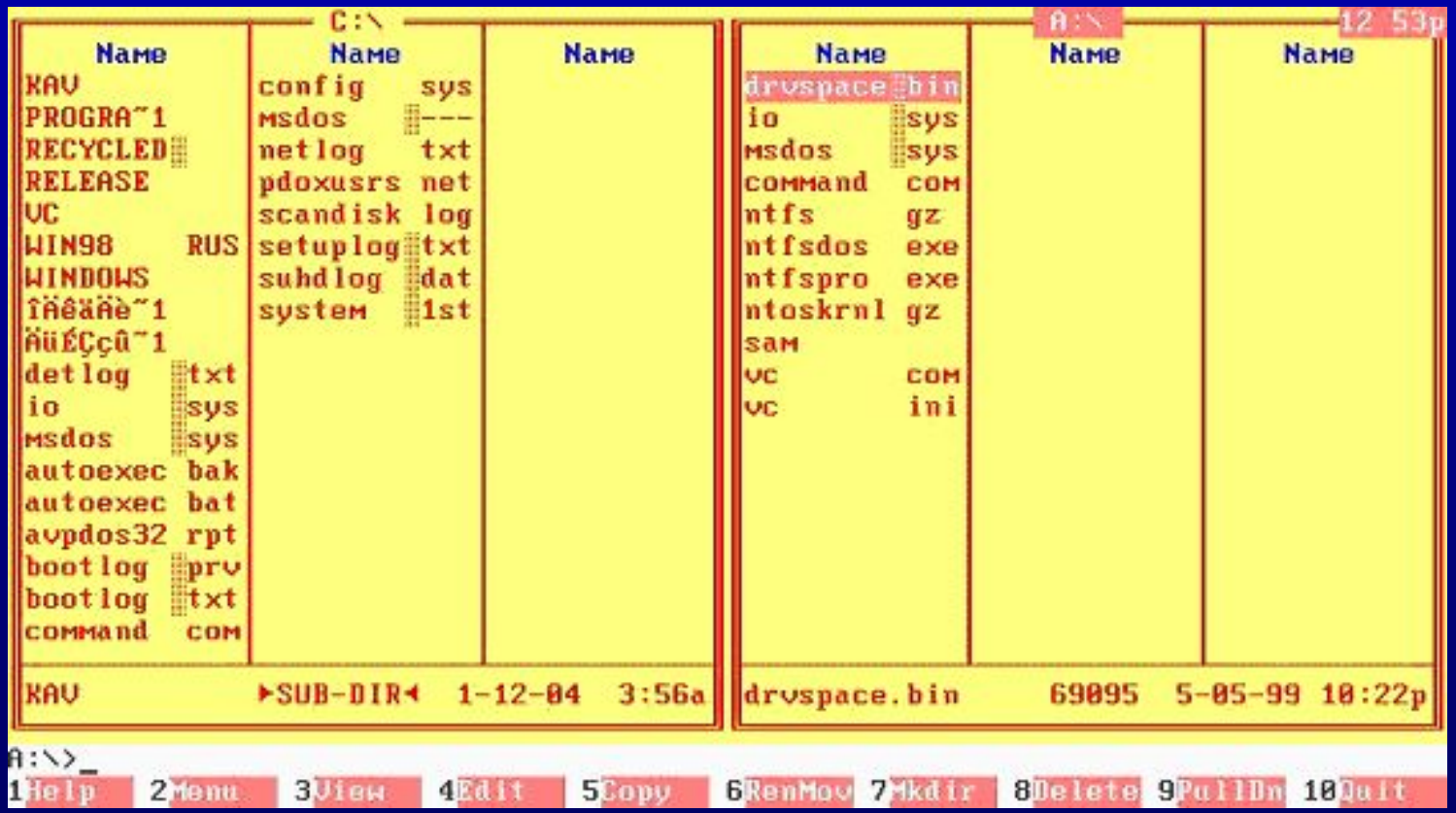
Смещение	Длина, байт	Описание
0x00	8	Неизвестно
0x08	8	Дата и время последней модификации учетной записи
0x10	8	Неизвестно
0x18	8	Дата и время создания учетной записи
0x20	8	Неизвестно
0x28	8	Дата и время последнего входа в систему
0x30	4	RID пользователя
0x34	4	Неизвестно
0x38	2	Флаги состояния учетной записи
0x3A	6	Неизвестно
0x40	2	Количество ошибок входа в систему
0x42	2	Общее количество входов в систему
0x44	12	Неизвестно, но у пользователей с правами администраторов первый байт всегда 1.

Флаги состояния учетной записи

- Значение Представление Описание
- 0x0001 01 00 Учетная запись отключена
- 0x0002 02 00 Требуется указание домашнего каталога
- 0x0004 04 00 Запретить смену пароля пользователем
- 0x0008 08 00 Неизвестно
- 0x0010 10 00 Обычная учетная запись
- 0x0020 20 00 Неизвестно
- 0x0040 40 00 Глобальная учетная запись
- 0x0080 80 00 Локальная учетная запись
- 0x0100 00 01 Доверенная запись
- 0x0200 00 02 Срок действия пароля не ограничен
- 0x0400 00 04 Учетная запись заблокирована

Средства анализа данных на NTFS-разделах

- Эмулятор NTFSDOS и NTFSDOSPro



Microsoft Windows xp

Чтобы начать работу, щелкните имя пользователя

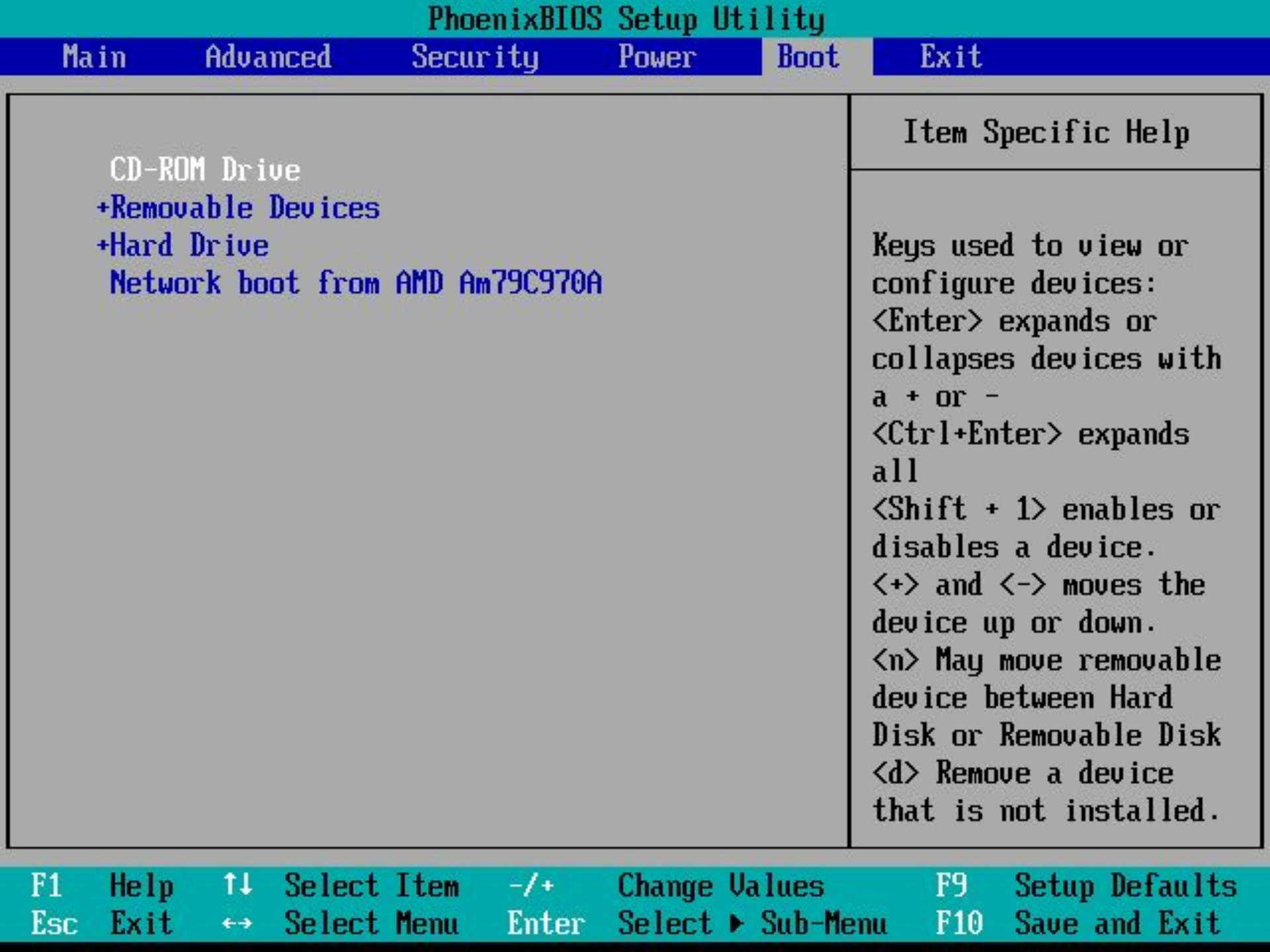
Администратор

Введите пароль

EN

Выключить компьютер

После входа в систему можно добавлять или изменять учетные записи.
Для этого в панели управления нужно выбрать "Учетные записи пользователей".


PhoenixBIOS Setup Utility
Main
Advanced
Security
Power
Boot
Exit
CD-ROM Drive
+Removable Devices
+Hard Drive
Network boot from AMD Am79C970A
Item Specific Help
Keys used to view or configure devices:
<Enter> expands or collapses devices with a + or -
<Ctrl+Enter> expands all
<Shift + 1> enables or disables a device.
<+> and <-> moves the device up or down.
<n> May move removable device between Hard Disk or Removable Disk
<d> Remove a device that is not installed.
F1 Help ↑↓ Select Item -/+ Change Values F9 Setup Defaults
Esc Exit ↔ Select Menu Enter Select ▸ Sub-Menu F10 Save and Exit


BART PE
created with PE-Builder
GO

Шифрующая файловая система EFS

- Шифрование отдельных файлов
- Шифрование каталогов (входящие файлы шифруются автоматически)

Шифрование с открытым ключом

- Пользователь: открытый и закрытый ключ
- Данные => симметричный алгоритм => ключ шифрования файла FEK (File Encryption Key), генерируется случайно

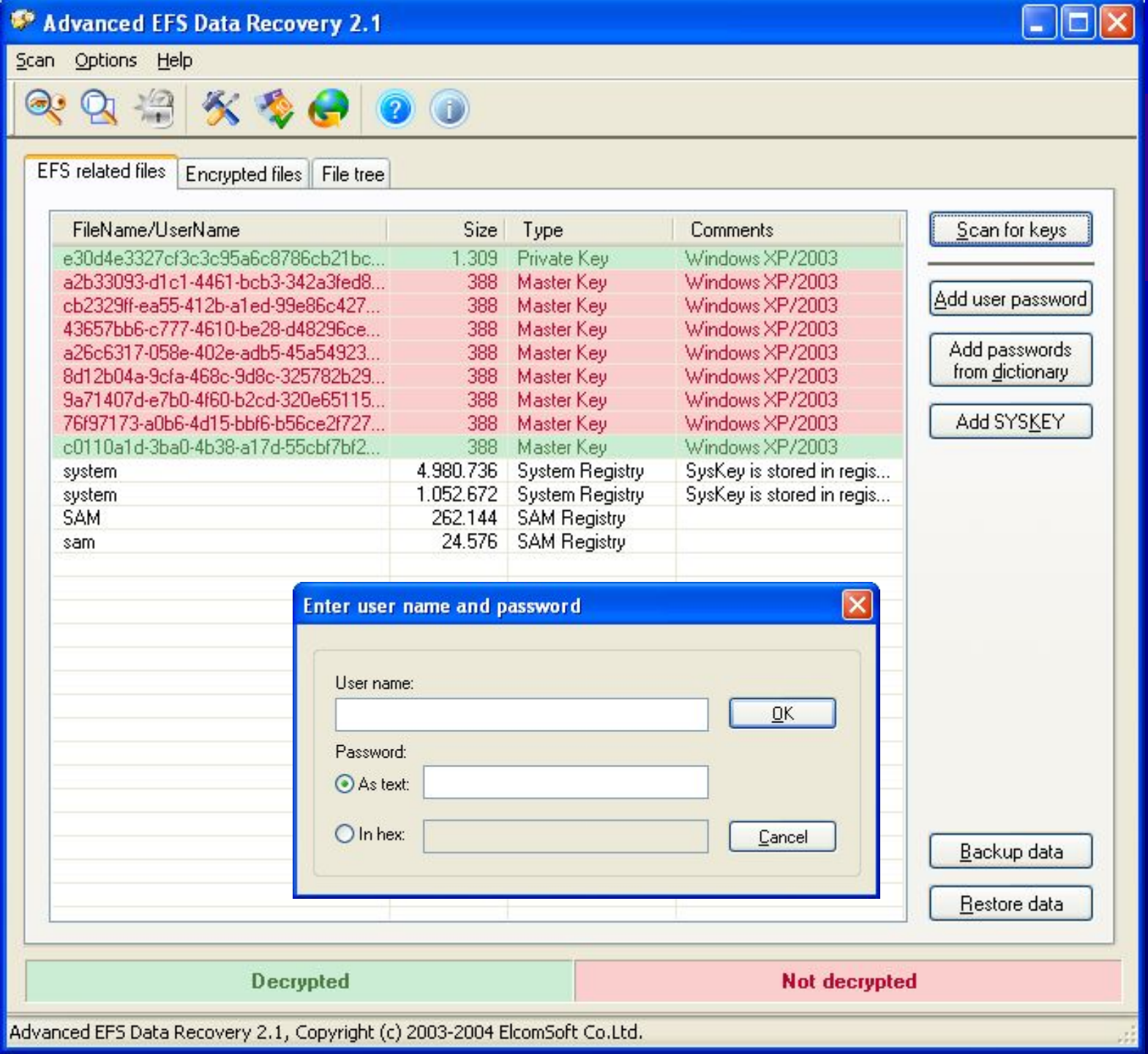
Шифрование с открытым ключом

- FEK => открытые ключи пользователей => список зашифрованных FEK => поле дешифрованных данных DDF
- FEK => открытые ключи агентов восстановления => список зашифрованных FEK => поле восстановления данных DRF

Расположение ключей

- ОС Windows XP
  - **C:\Documents and Settings\Имя_пользователя \Application Data**
- ОС Windows 7
  - **C:\Users\Appdata\Roaming**

- Сертификат открытого ключа
- \Microsoft\SystemCertificates\My\Certificates
- Закрытый ключ пользователя
- \Microsoft\Crypto\RSA \Идентификатор пользователя
- Файл блокировки
- \Microsoft\Protect\ Идентификатор пользователя


Advanced EFS Data Recovery 2.1
Scan Options Help
EFS related files
Encrypted files
File tree
FileName/UserName Size Type Comments
e30d4e3327cf3c3c95a6c8786cb21bc... 1.309 Private Key Windows XP/2003
a2b33093-d1c1-4461-bcb3-342a3fed8... 388 Master Key Windows XP/2003
cb2329ff-ea55-412b-a1ed-99e86c427... 388 Master Key Windows XP/2003
43657bb6-c777-4610-be28-d48296ce... 388 Master Key Windows XP/2003
a26c6317-058e-402e-adb5-45a54923... 388 Master Key Windows XP/2003
8d12b04a-9cfa-468c-9d8c-325782b29... 388 Master Key Windows XP/2003
9a71407d-e7b0-4f60-b2cd-320e65115... 388 Master Key Windows XP/2003
76f97173-a0b6-4d15-bbf6-b56ce2f727... 388 Master Key Windows XP/2003
c0110a1d-3ba0-4b38-a17d-55cbf7bf2... 388 Master Key Windows XP/2003
system 4.980.736 System Registry SysKey is stored in regis...
system 1.052.672 System Registry SysKey is stored in regis...
SAM 262.144 SAM Registry
sam 24.576 SAM Registry
Scan for keys
Add user password
Add passwords from dictionary
Add SYSKEY
Backup data
Restore data
Enter user name and password
User name:
OK
Password:
As text:
In hex:
Cancel
Decrypted
Not decrypted
Advanced EFS Data Recovery 2.1, Copyright (c) 2003-2004 ElcomSoft Co.Ltd.

Дополнительные замечания

- Временный файл efs0.tmp
- Не подлежат шифрованию файлы в системном каталоге
- Для расшифрования файлов требуется пароль пользователя, их зашифровавшего
- Утилита AEFSDR
- Создание AB – cipher /R

Хранение парольной информации

Аутентификация пользователей

Имя +

- Пароль
- Ключевая дискета
- Жетон
- Психобиофизические характеристики человека

Пароль

Мах длина пароля - 14 символов (128)

Расположение БД SAM

- Куст реестра SAM в HKEY_LOCAL_MACHINE
- Winnt\System32\Config\sam - текущая база данных
- Winnt\Repair\sam - копия, создается при выполнении резервного копирования
- ERD - диск аварийного восстановления

Хранение парольной информации в БД SAM

- Имя учетной записи
- ID - в открытом виде
- Пароль - в зашифрованном виде:
  - Пароль Windows NT
  - Пароль LAN Manager

Имя	SID	NT hash	Lanman hash
User1	s-1…-1010		
User2	s-1…-1011		

Параметр *V*

- 0x00 Элемент неизвестного назначения
- 0x0C Индекс имени пользователя
- 0x18 Индекс полного имени
- ……..
- 0x84 Индекс времени, разрешенного для регистрации (обычно содержит 168 (0xA8) бит – по одному на каждый час недели)
- 0x90 Элемент неизвестного назначения
- 0x9C Индекс зашифрованного пароля LAN Manager
- 0xA8 Индекс зашифрованного пароля Windows NT
- 0xB4 Индекс предыдущего зашифрованного пароля Windows NT
- 0xC0 Индекс предыдущего зашифрованного пароля LAN Manager

Шифрование парольной информации

Шифрование паролей Windows NT

OWF -Необратимая функция, RSA MD4

DES: ключ - RID пользователя

БД SAM

Имя	SID	NT hash	Lanman hash
User1	s-1…-1010	16 байт хэш	
User2	s-1…-1011	16 байт хэш	

Локальная регистрация

OWF -Необратимая функция, RSA MD4

DES: ключ - RID пользователя

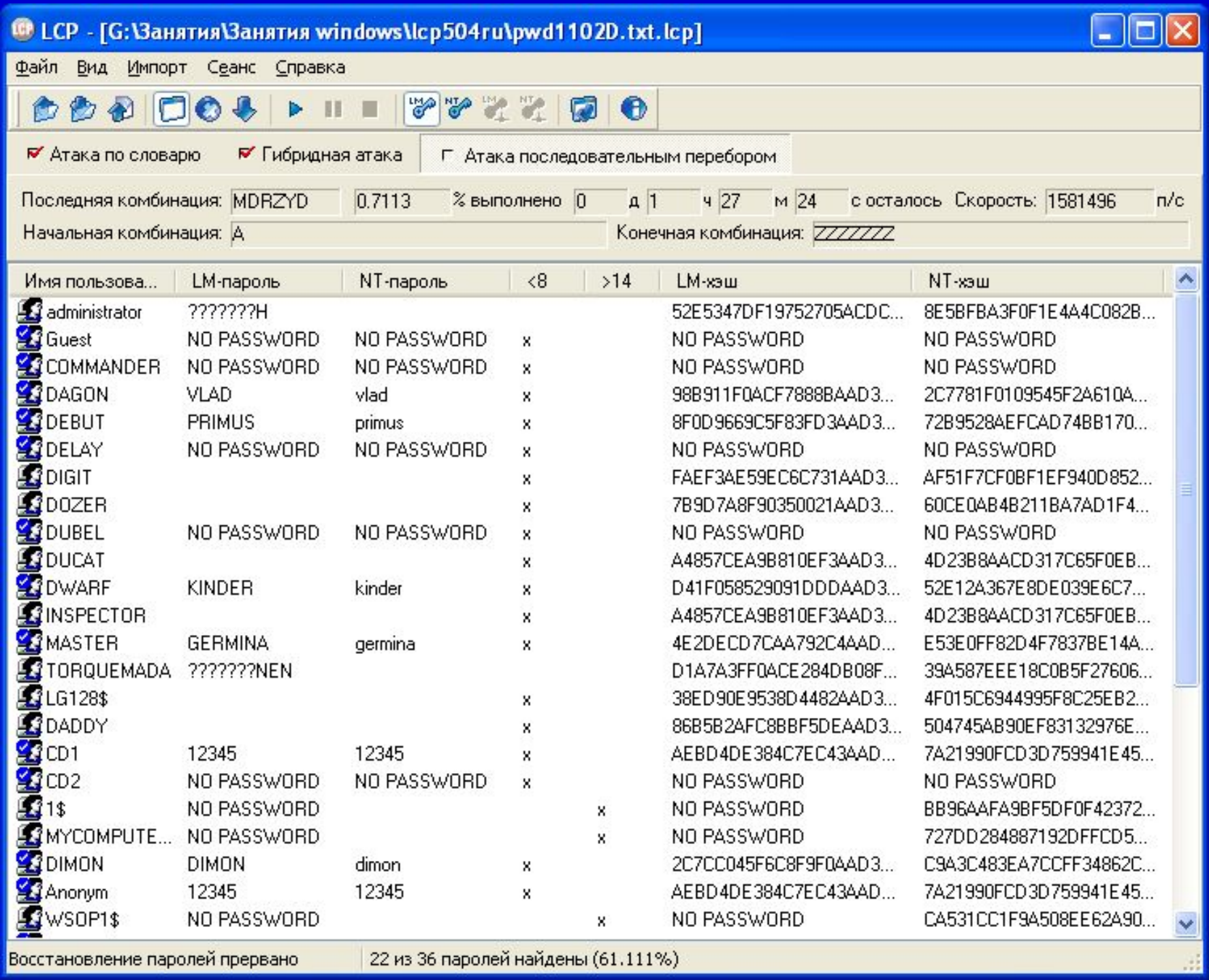
Шифрование паролей LAN Manager

Если длина пароля <= 7 символов, то 2-ая половина хеша известна - AAD3B435B51404EE

DES: ключ - 7 символов пароля, шифруется «магическое» число

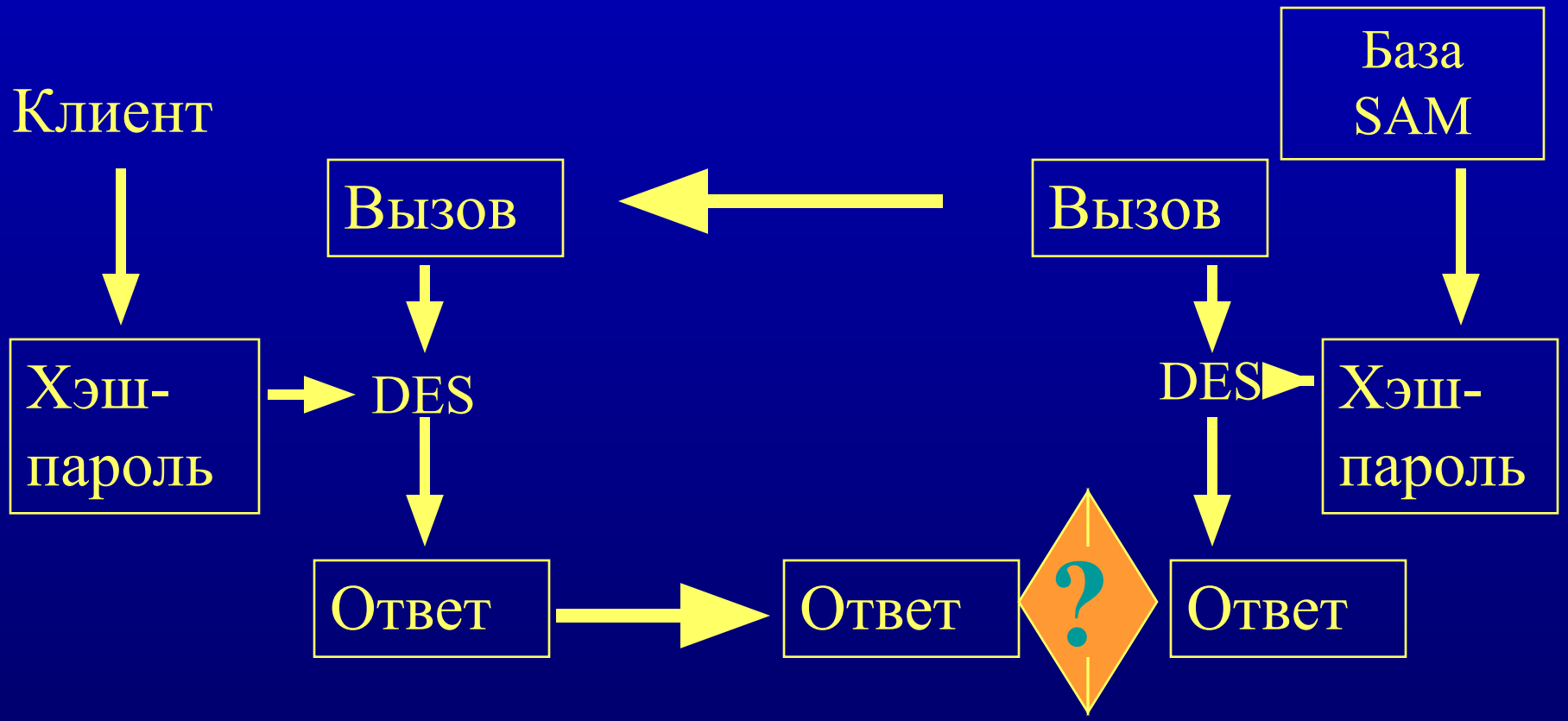
БД SAM

Имя	SID	NT hash	Lanman hash
User1	s-1…-1010	16 байт хэш	8+8 байт хэш
User2	s-1…-1011	16 байт хэш	8+8 байт хэш


LCP - [G:\Занятия\Занятия windows\lcp504ru\pwd1102D.txt.lcp]
Файл Вид Импорт Сеанс Справка
Атака по словарю
Гибридная атака
Атака последовательным перебором
Последняя комбинация: MDRZYD
0.7113 % выполнено
0 д 1 ч 27 м 24 с осталось
Скорость: 1581496 п/с
Начальная комбинация: A
Конечная комбинация: ZZZZZZZ
Имя пользова... LM-пароль NT-пароль <8 >14 LM-хэш NT-хэш
administrator ???????H 52E5347DF19752705ACDC... 8E5BFBA3F0F1E4A4C082B...
Guest NO PASSWORD NO PASSWORD x NO PASSWORD NO PASSWORD
COMMANDER NO PASSWORD NO PASSWORD x NO PASSWORD NO PASSWORD
DAGON VLAD vlad x 98B911F0ACF7888BAAD3... 2C7781F0109545F2A610A...
DEBUT PRIMUS primus x 8F0D9669C5F83FD3AAD3... 72B9528AEFCAD74BB170...
DELAY NO PASSWORD NO PASSWORD x NO PASSWORD NO PASSWORD
DIGIT x FAEF3AE59EC6C731AAD3... AF51F7CF0BF1EF940D852...
DOZER x 7B9D7A8F90350021AAD3... 60CE0AB4B211BA7AD1F4...
DUBEL NO PASSWORD NO PASSWORD x NO PASSWORD NO PASSWORD
DUCAT x A4857CEA9B810EF3AAD3... 4D23B8AACD317C65F0EB...
DWARF KINDER kinder x D41F058529091DDDAAD3... 52E12A367E8DE039E6C7...
INSPECTOR x A4857CEA9B810EF3AAD3... 4D23B8AACD317C65F0EB...
MASTER GERMINA germina x 4E2DECD7CAA792C4AAD... E53E0FF82D4F7837BE14A...
TORQUEMADA ???????NEN D1A7A3FF0ACE284DB08F... 39A587EEE18C0B5F27606...
LG128$ x 38ED90E9538D4482AAD3... 4F015C6944995F8C25EB2...
DADDY x 86B5B2AFC8BBF5DEAAD3... 504745AB90EF83132976E...
CD1 12345 12345 x AEBD4DE384C7EC43AAD... 7A21990FCD3D759941E45...
CD2 NO PASSWORD NO PASSWORD x NO PASSWORD NO PASSWORD
1$ NO PASSWORD x NO PASSWORD BB96AAFA9BF5DF0F42372...
MYCOMPUTE... NO PASSWORD x NO PASSWORD 727DD284887192DFFCD5...
DIMON DIMON dimon x 2C7CC045F6C8F9F0AAD3... C9A3C483EA7CCFF34862C...
Anonym 12345 12345 x AEBD4DE384C7EC43AAD... 7A21990FCD3D759941E45...
WSOP1$ NO PASSWORD x NO PASSWORD CA531CC1F9A508EE62A90...
Восстановление паролей прервано
22 из 36 паролей найдены (61.111%)

Процесс аутентификации пользователей по сети

Проверка пароля



Шифрование пароля

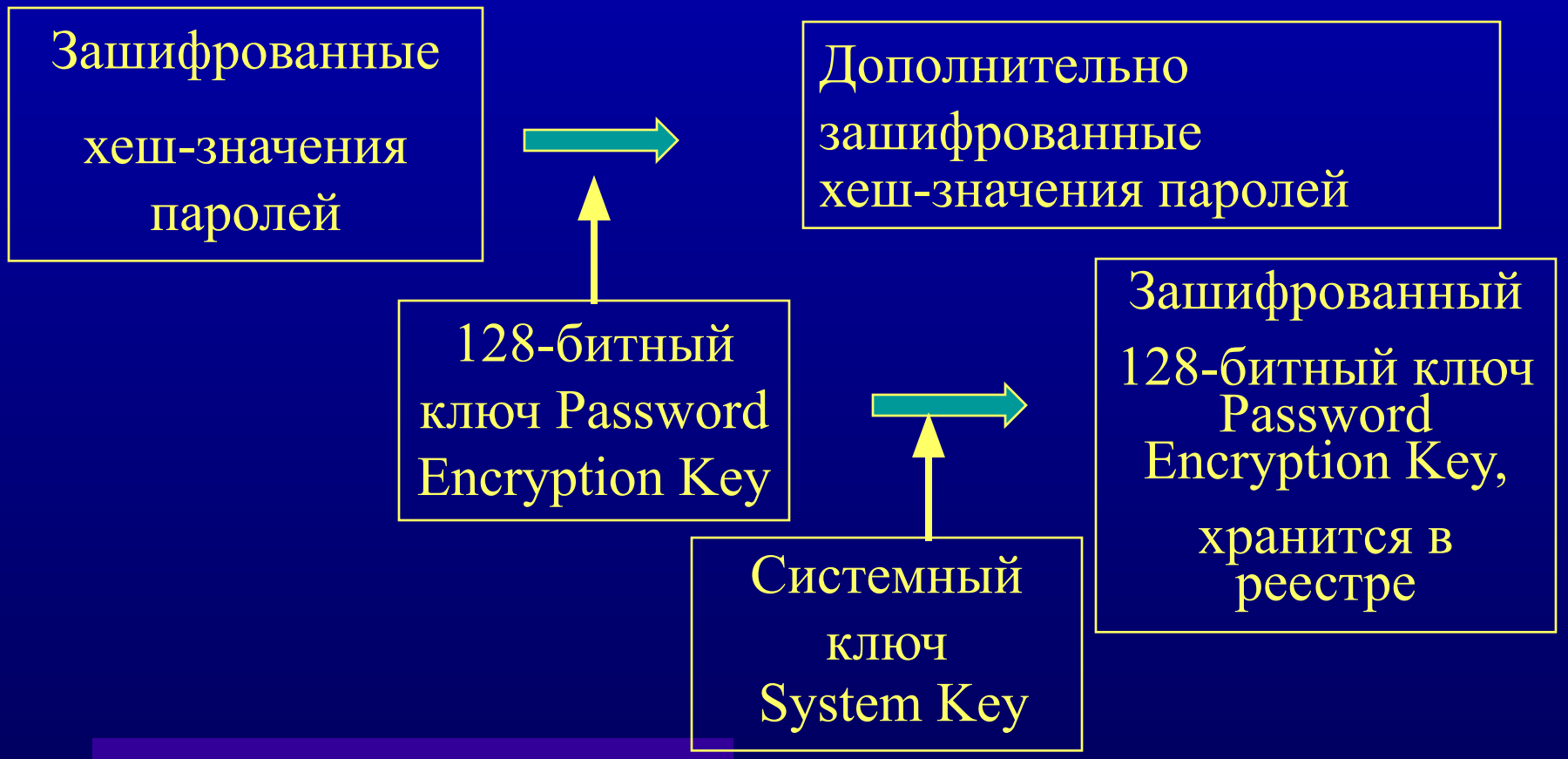
- Сервер передает 8-байтовый вызов
- Клиент шифрует (DES) вызов, используя в качестве ключа 16-байтовый хешированный пароль
- Ответ клиента - структура длиной 24 байта
- В случае диалекта NT LM 0.12 клиент передает два «ответа» (для NT и LANMAN) - общей длиной 48 байт

Ключевые моменты

- Ни открытый пароль, ни хеш пароля по сети не передаются
- Для НСД знания пароля не нужно - нужно лишь знание хеш-значения
- По передаваемым по сети данным (Вызов -Ответ) нельзя расшифровать ни сам пароль, ни его хеш-значение
- Перехватив ответ, невозможно использовать его для открытия сеанса, так как вызов генерируется снова для нового соединения
- Данные, передаваемые в ходе сеанса, не шифруются

Дополнительное шифрование хешированных паролей в БД SAM

- Программа Syskey



Способы хранения системного ключа

- В реестре компьютера
- На отдельной дискете
- Ключ не хранится, а вычисляется из пароля, вводимого при загрузке

Атаки на пароли

Атаки на БД SAM

- Цели:
- извлечение хешированных паролей
  - для подбора текстового пароля
  - для сетевого соединения без подбора текстового пароля
- модификация SAM
  - подмена пароля пользователя
  - добавление нового пользователя и т.п.

Способы получения базы SAM

- Загрузка с DOS-дискеты с использованием эмуляторов NTFS
  - NTFSDOS.exe
  - NtRecover.exe
- Получение резервной копии SAM с ERD-диска, магнитных лент, каталога Winnt\repair
- Перехват «вызова» и «ответа» и выполнение полного перебора

Подбор пароля по HASH

- Brute force attack - перебор всех комбинаций символов из заданного набора
- Словарь
  - данные о пользователе
  - «хитрости» и «глупости»
    - слова-наоборот
    - qwerty, 12345
    - IVAN
    - пароль = ID

Количество комбинаций символов

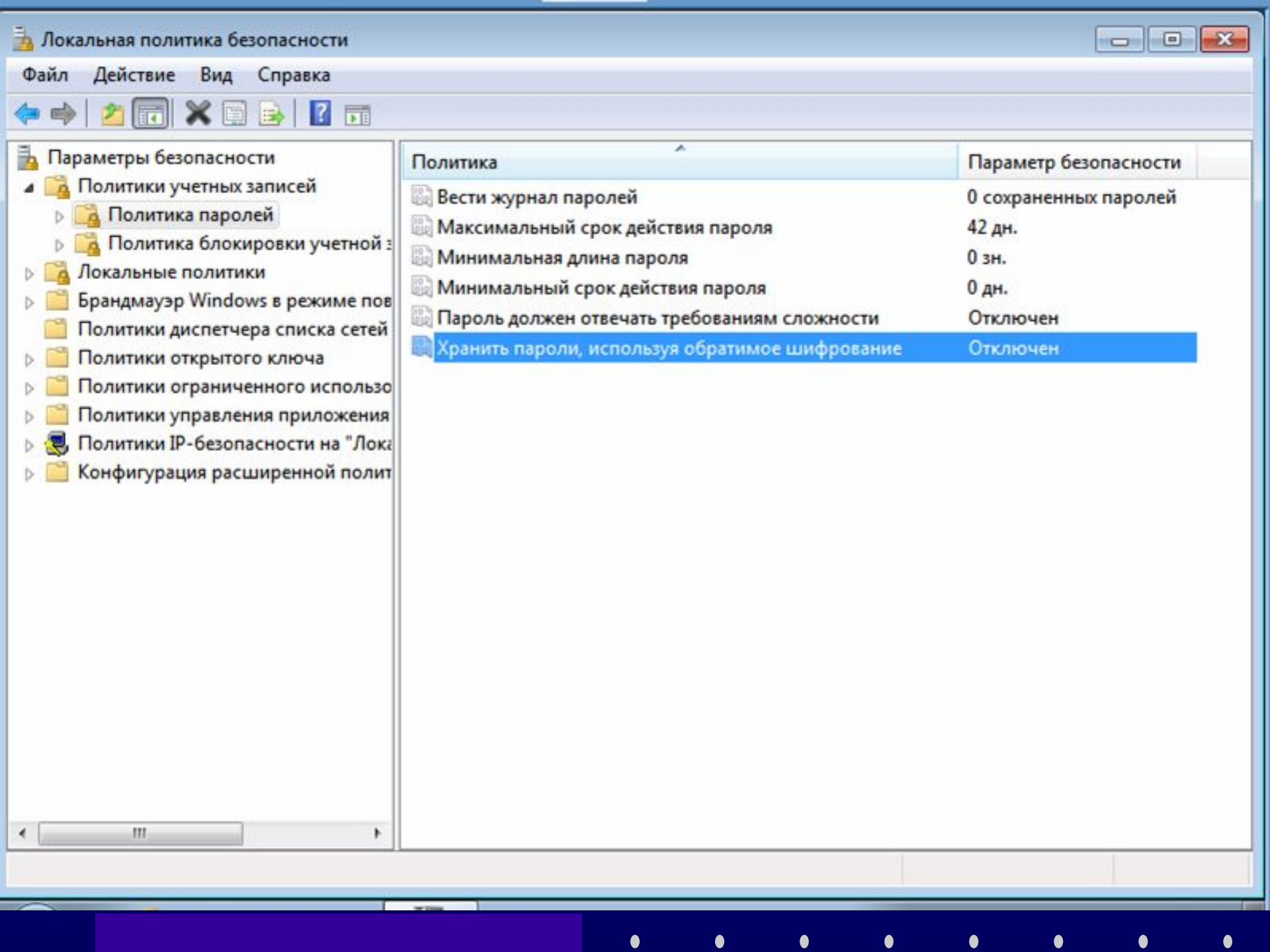
1 сутки

10 суток

Длина пароля	A-Z	A-Z, 0-9	A-Z, a-z, 0-9
5	12 млн	60,5 млн	915 млн
6	310 млн	2 млрд	57 млрд
7	8 млрд	80 млрд	3,5 трлн
8	210 млрд	3 трлн	218 трлн

Что дает hash LAN Manager?

- Недостаточная устойчивость к взлому
  - символы ВЕРХНЕГО регистра
  - две половины по 7 символов
- Все комбинации перебираются за 10 суток
- Если известен пароль в верхнем регистре, то вариацией букв (верх/нижн) получаем пароль Windows NT
- Отключен в Windows 7


Локальная политика безопасности
Файл
Действие
Вид
Справка
Параметры безопасности
Политики учетных записей
Политика паролей
Политика блокировки учетной
Локальные политики
Брандмауэр Windows в режиме пов
Политики диспетчера списка сетей
Политики открытого ключа
Политики ограниченного использо
Политики управления приложения
Политики IP-безопасности на "Лока
Конфигурация расширенной полит
Политика
Параметр безопасности
Вести журнал паролей
0 сохраненных паролей
Максимальный срок действия пароля
42 дн.
Минимальная длина пароля
0 зн.
Минимальный срок действия пароля
0 дн.
Пароль должен отвечать требованиям сложности
Отключен
Хранить пароли, используя обратимое шифрование
Отключен

Механизм LAN Manager аутентификации в сети

256

65535

Клиент

8 байт «вызов» 0001020304050607

Сервер

16 байт hash + 5 нулей = 21 байт

C2341A8AA1E7665F AAD3B435B51404EE

C2341A8AA1E7665F AAD3B435B51404EE 0000000000

7 байт | 7 байт | 7 байт

C2341A8AA1E766 | 5FAAD3B435B514 | 04EE0000000000

8 байт DES Key | 8 байт DES Key | 8 байт DES Key

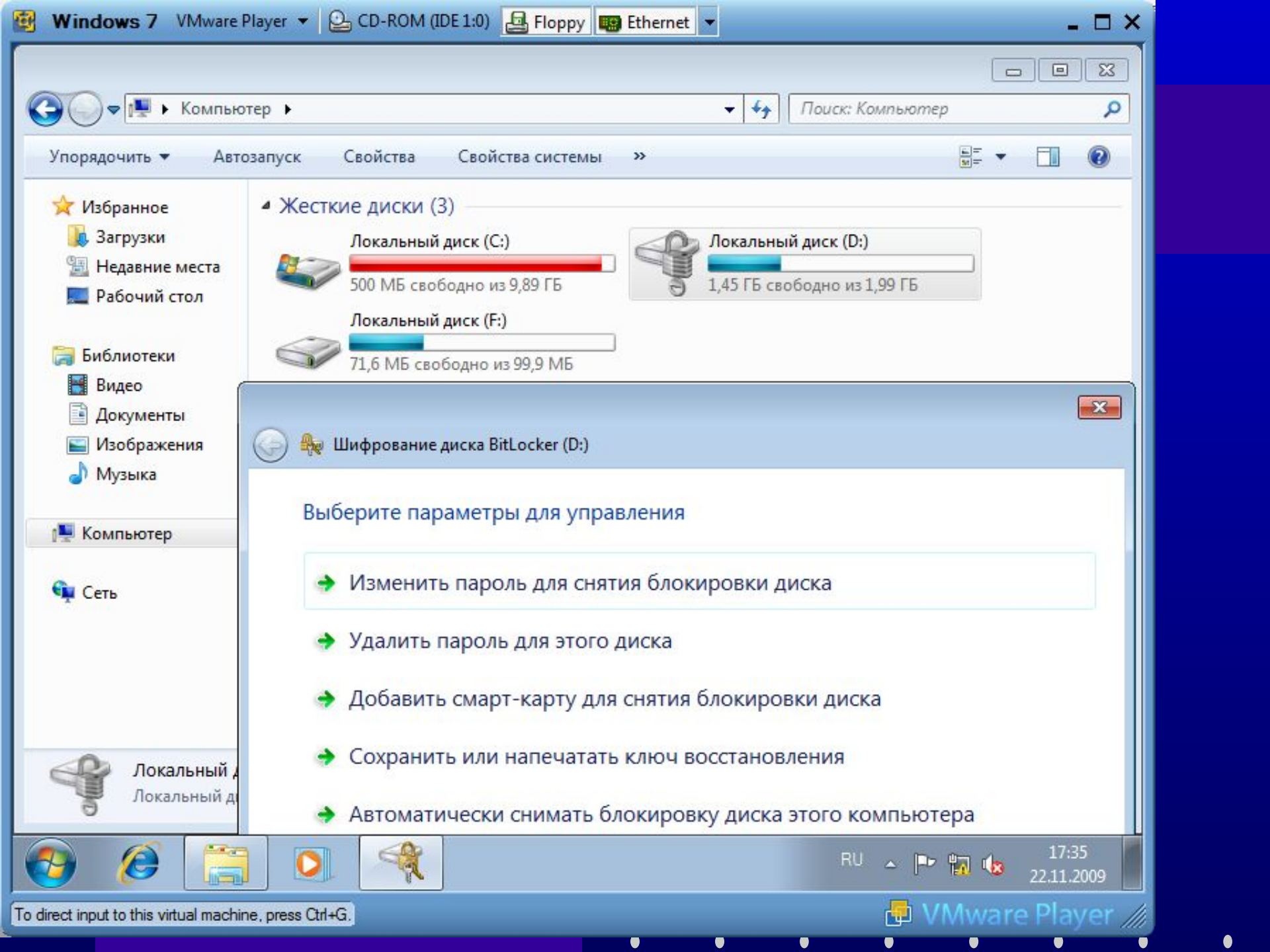
Шифруем «вызов» | Шифруем «вызов» | Шифруем «вызов»

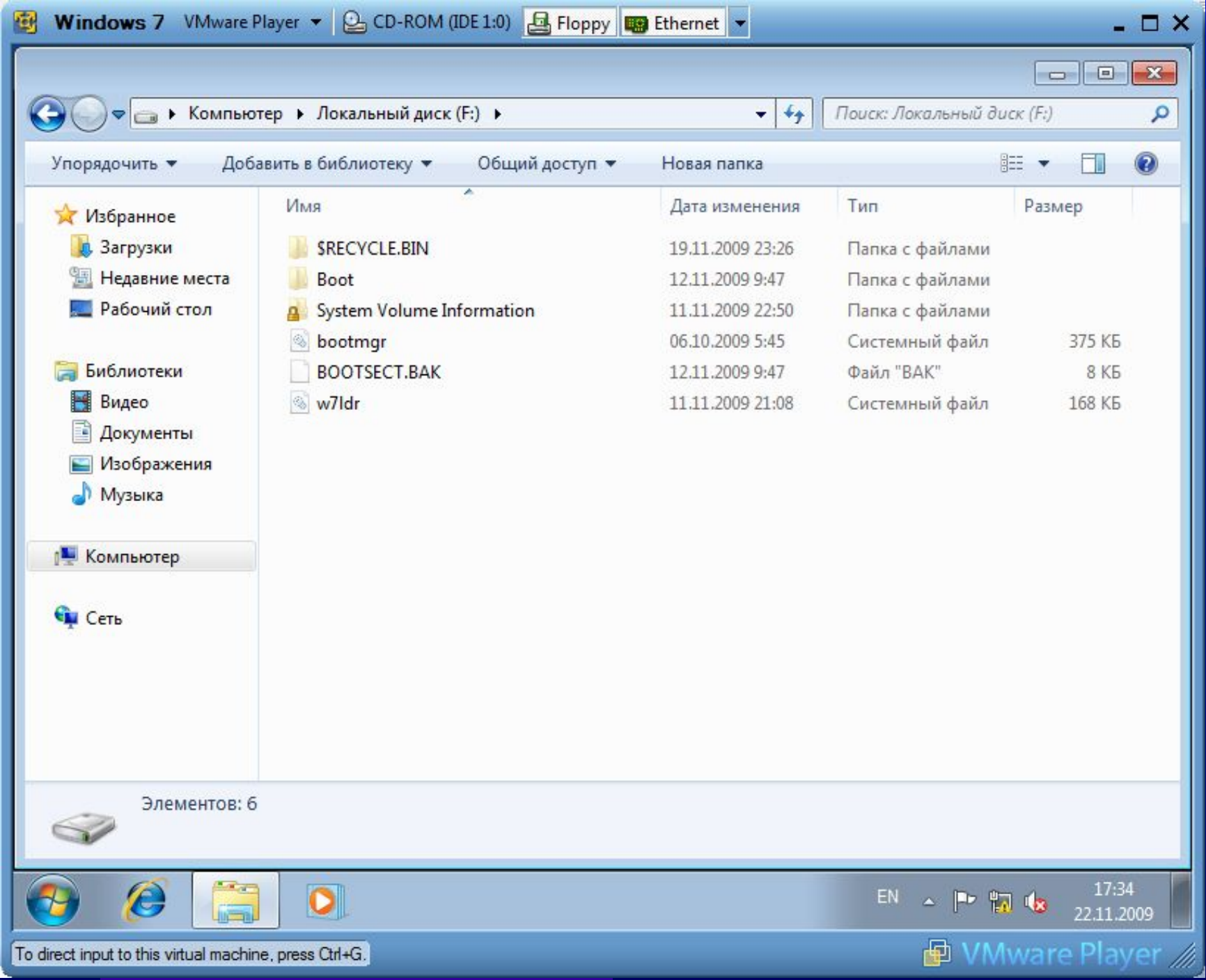
AAAAAAAAAAAAAAAA | BBBBBBBBBBBBBBBB | CCCCCCCCCCCCCCCC

«Ответ»

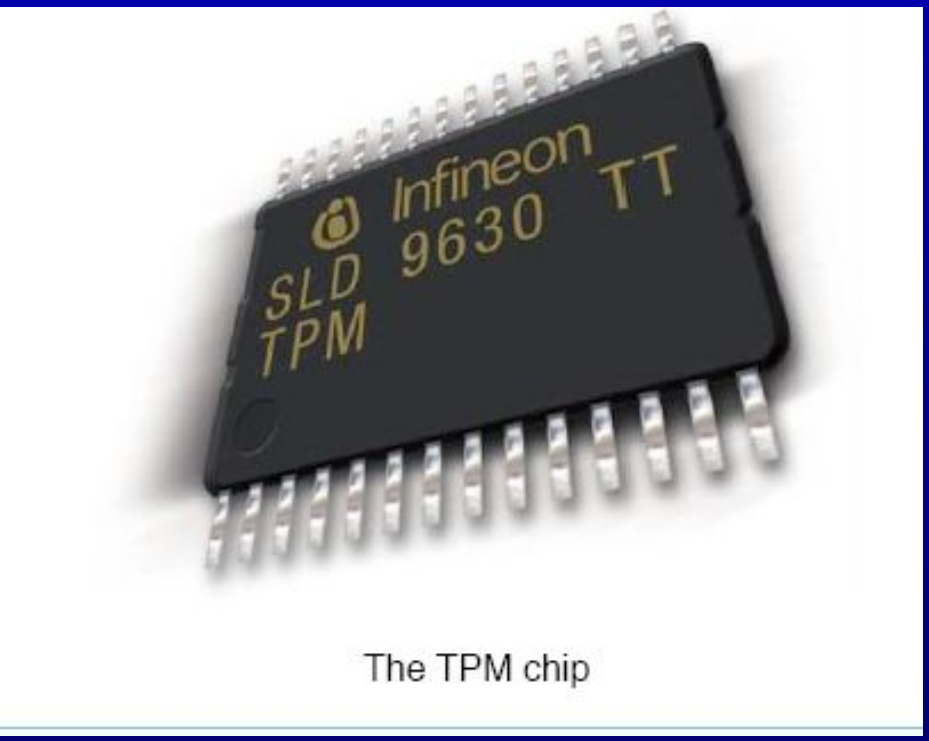
BitLocker drive encryption

- Версии Vista, 7
  - Starter, Home Basic, Home Premium, Business, Ultimate, Enterprise
- Посекторное шифрование всего тома ОС алгоритмом AES (128 бит) кроме
  - загрузочного сектора;
  - поврежденных секторов;
  - метаданных тома.
- Проверка целостности загрузочных компонентов до запуска ОС


Windows 7
VMware Player
CD-ROM (IDE 1:0)
Floppy
Ethernet
Компьютер
Поиск: Компьютер
Упорядочить
Автозапуск
Свойства
Свойства системы
Избранное
Загрузки
Недавние места
Рабочий стол
Библиотеки
Видео
Документы
Изображения
Музыка
Компьютер
Сеть
Жесткие диски (3)
Локальный диск (C:)
500 МБ свободно из 9,89 ГБ
Локальный диск (D:)
1,45 ГБ свободно из 1,99 ГБ
Локальный диск (F:)
71,6 МБ свободно из 99,9 МБ
Шифрование диска BitLocker (D:)
Выберите параметры для управления
Изменить пароль для снятия блокировки диска
Удалить пароль для этого диска
Добавить смарт-карту для снятия блокировки диска
Сохранить или напечатать ключ восстановления
Автоматически снимать блокировку диска этого компьютера
RU
17:35
22.11.2009
To direct input to this virtual machine, press Ctrl+G.
VMware Player


Windows 7
VMware Player
CD-ROM (IDE 1:0)
Floppy
Ethernet
Компьютер ▸ Локальный диск (F:) ▸
Поиск: Локальный диск (F:)
Упорядочить
Добавить в библиотеку
Общий доступ
Новая папка
Избранное
Загрузки
Недавние места
Рабочий стол
Библиотеки
Видео
Документы
Изображения
Музыка
Компьютер
Сеть
Имя
Дата изменения
Тип
Размер
$RECYCLE.BIN 19.11.2009 23:26 Папка с файлами
Boot 12.11.2009 9:47 Папка с файлами
System Volume Information 11.11.2009 22:50 Папка с файлами
bootmgr 06.10.2009 5:45 Системный файл 375 КБ
BOOTSECT.BAK 12.11.2009 9:47 Файл "BAK" 8 КБ
w7ldr 11.11.2009 21:08 Системный файл 168 КБ
Элементов: 6
EN
17:34
22.11.2009
To direct input to this virtual machine, press Ctrl+G.
VMware Player

Доверенный платформенный модуль (TPM — Trusted Platform Module)



The TPM chip

- Хранение «предохранителя» ключа шифрования тома
- Хранение регистров конфигурации платформы (Platform Configuration Registers, PCR)

Архитектура ключей BitLocker

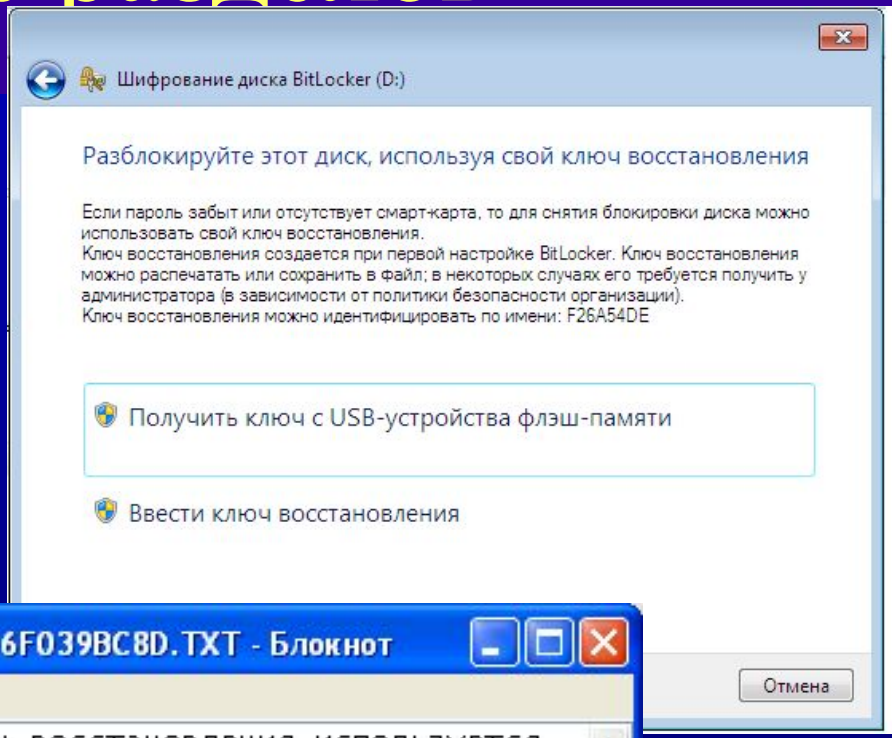
- Ключ шифрования тома (full-volume encryption key, FVEK) зашифрован с помощью
- Основного ключа тома (volume master key, VMK), зашифрованного
- Предохранителями (одним или несколькими)

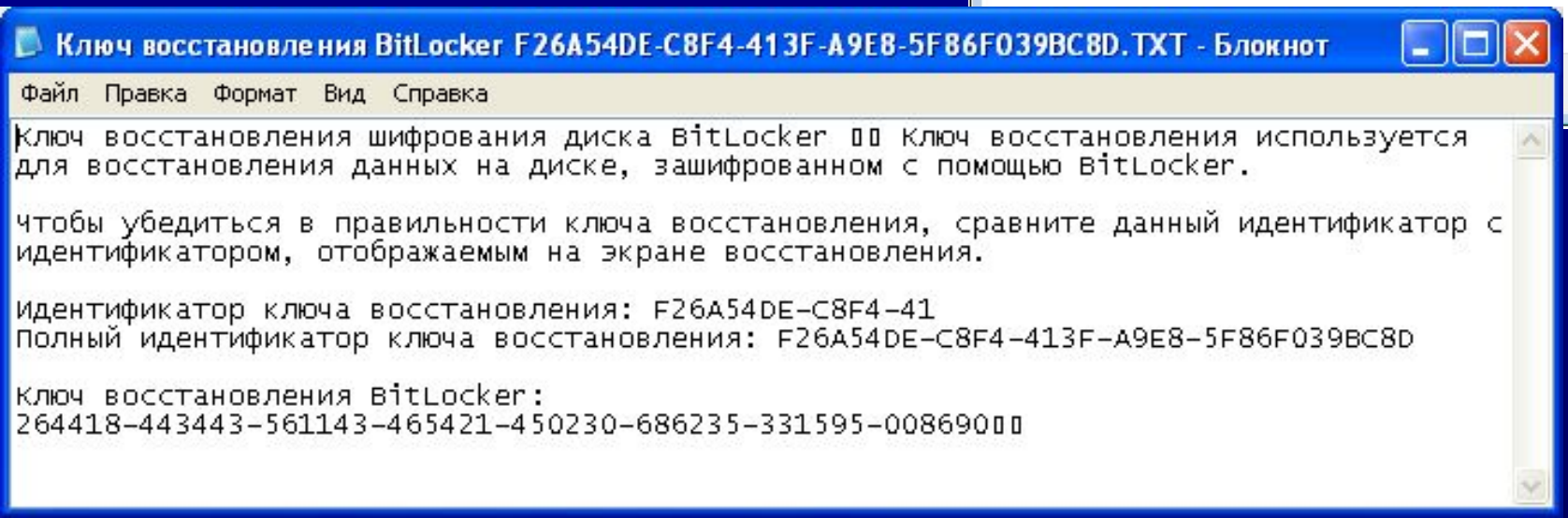
Типы предохранителей

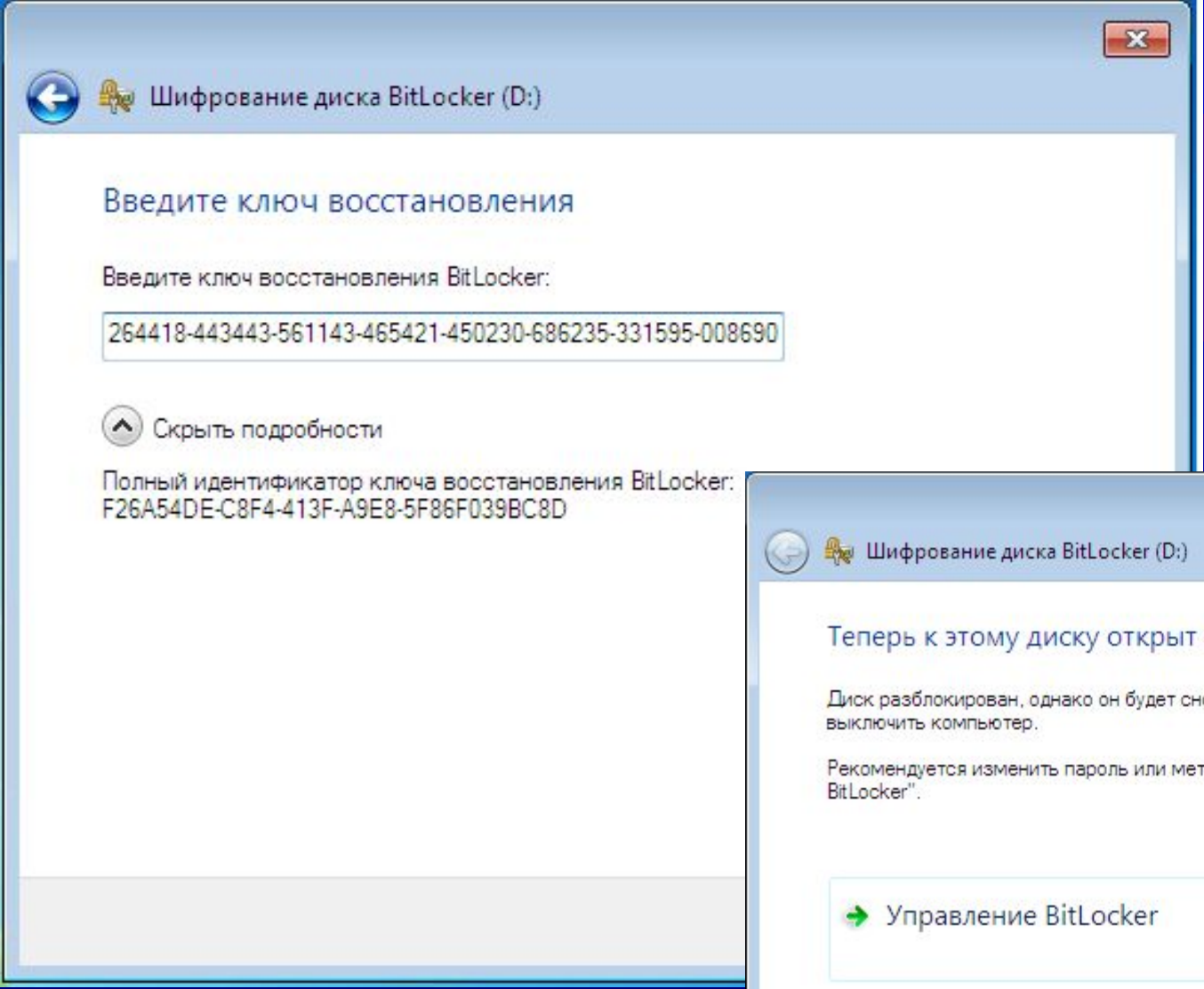
- TPM
- USB-накопитель (ключ запуска)
- Незашифрованный ключ на диске (при отключении BitLocker)

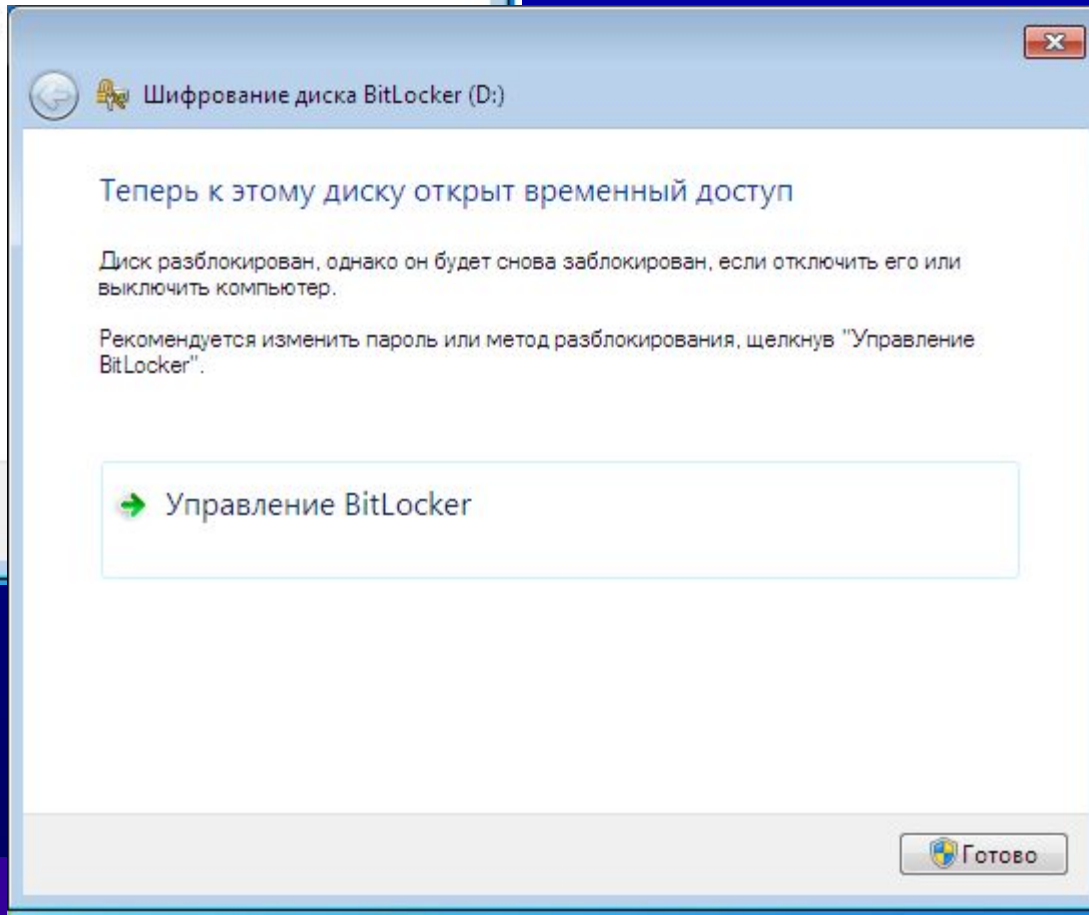
Шифрование разделов

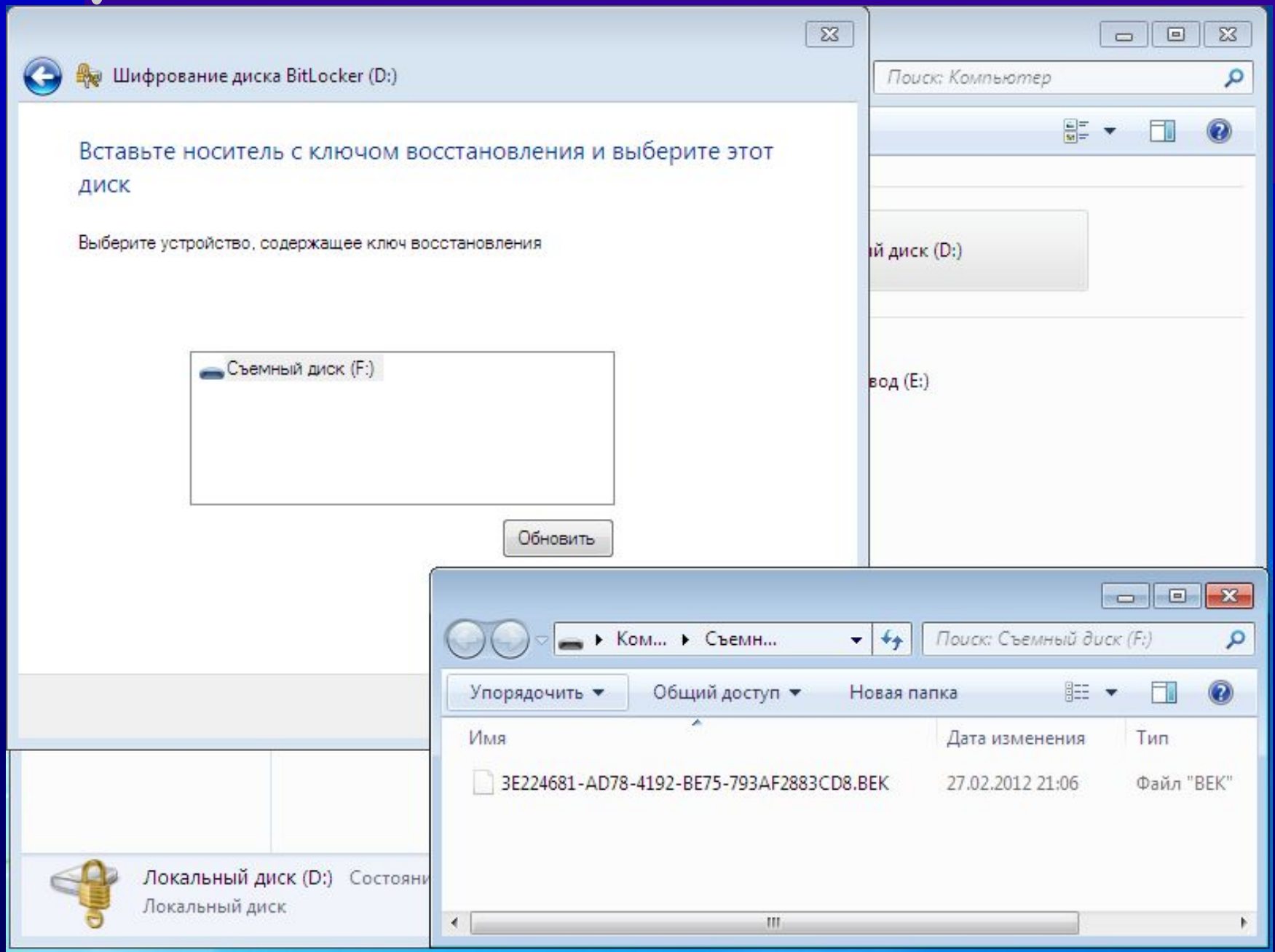
- Для системного раздела
  - TPM
  - USB-накопитель (ключ запуска)
  - Ключ восстановления (48 цифр)
- Для пользовательского раздела
  - Пароль (не менее 8 символов)
  - Смарт-карта
  - Ключ восстановления (48 цифр)





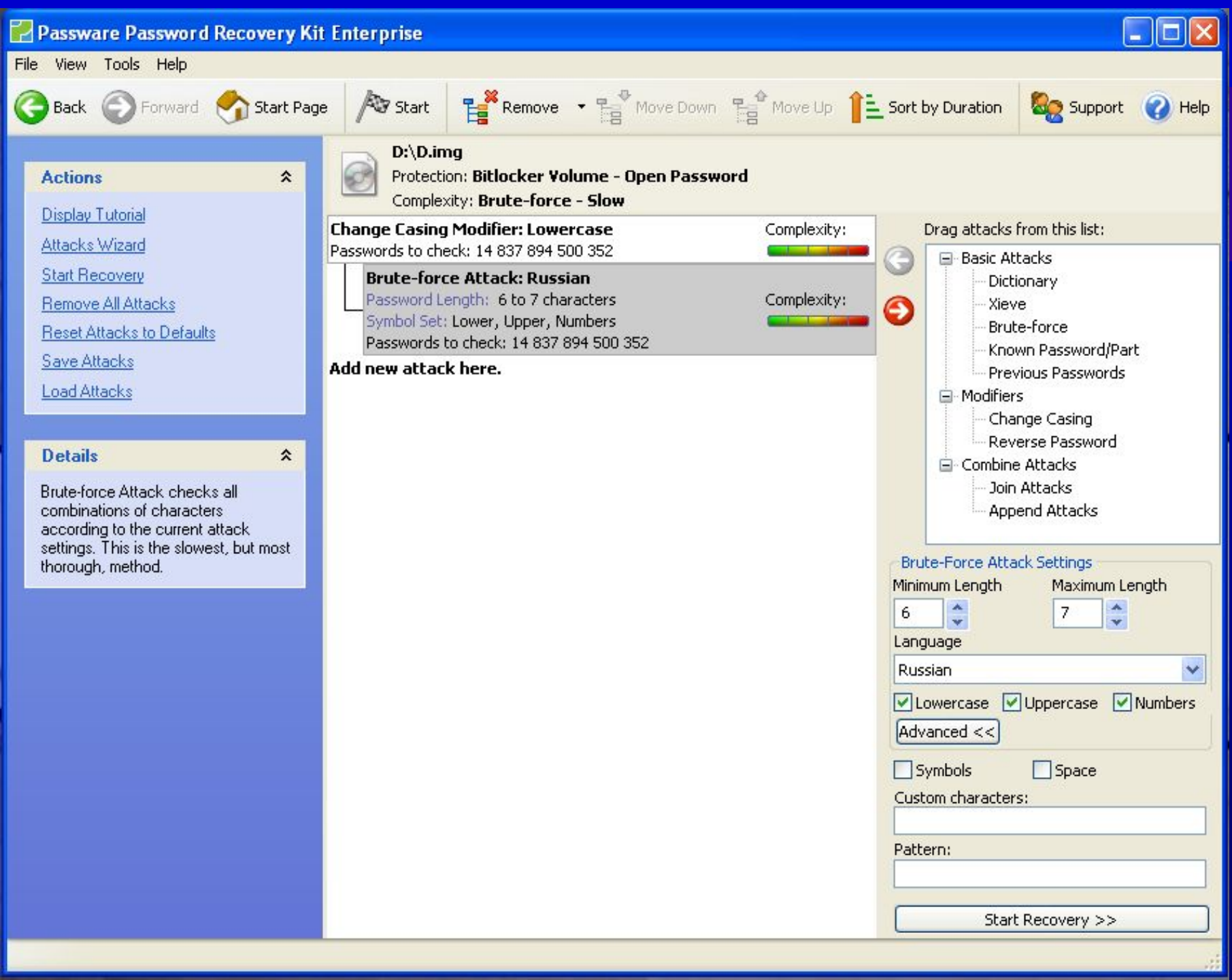

Шифрование диска BitLocker (D:)
Введите ключ восстановления
Введите ключ восстановления BitLocker:
264418-443443-561143-465421-450230-686235-331595-008690
Скрыть подробности
Полный идентификатор ключа восстановления BitLocker:
F26A54DE-C8F4-413F-A9E8-5F86F039BC8D

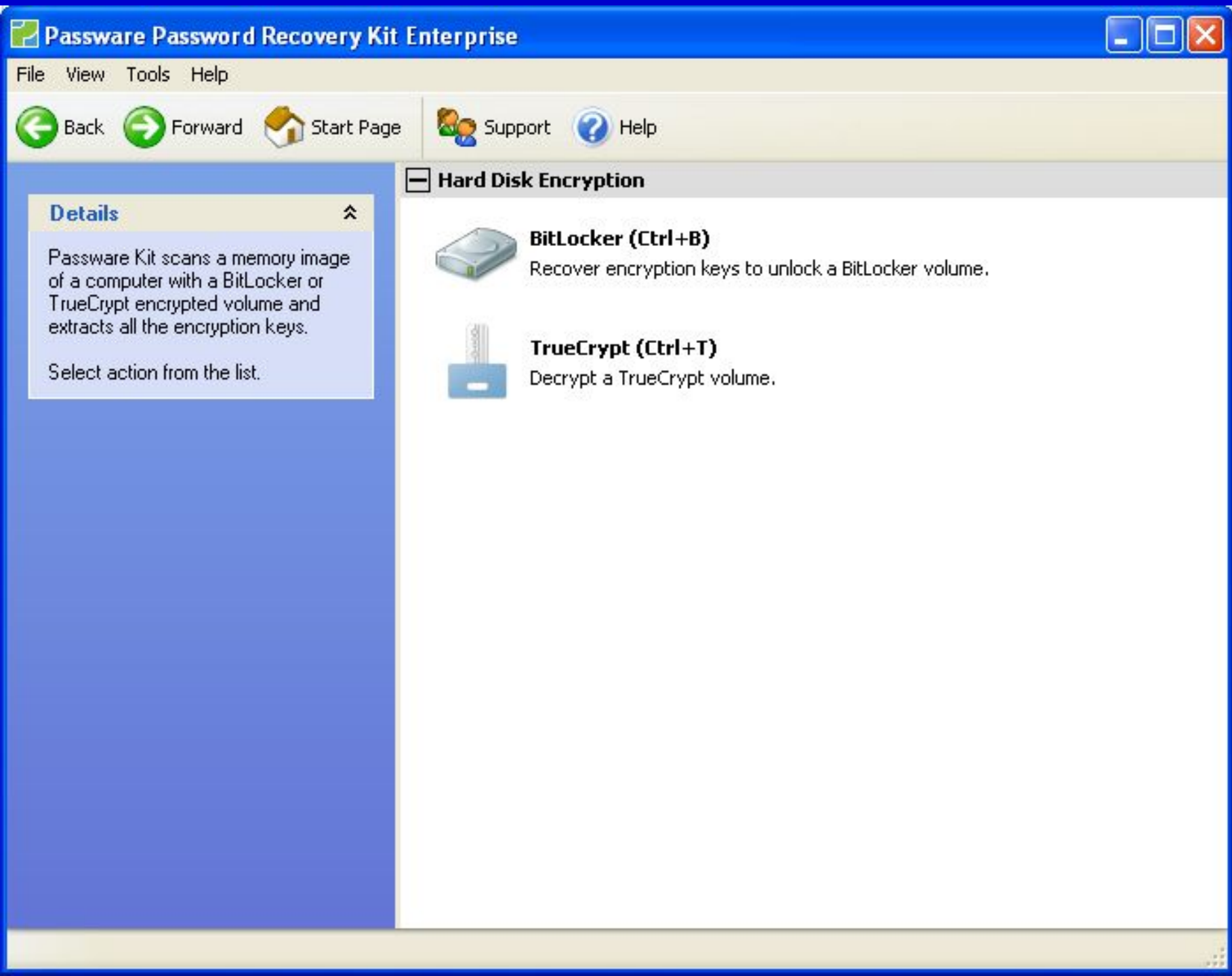

Шифрование диска BitLocker (D:)
Теперь к этому диску открыт временный доступ
Диск разблокирован, однако он будет снова заблокирован, если отключить его или выключить компьютер.
Рекомендуется изменить пароль или метод разблокирования, щелкнув "Управление BitLocker".
Управление BitLocker
Готово

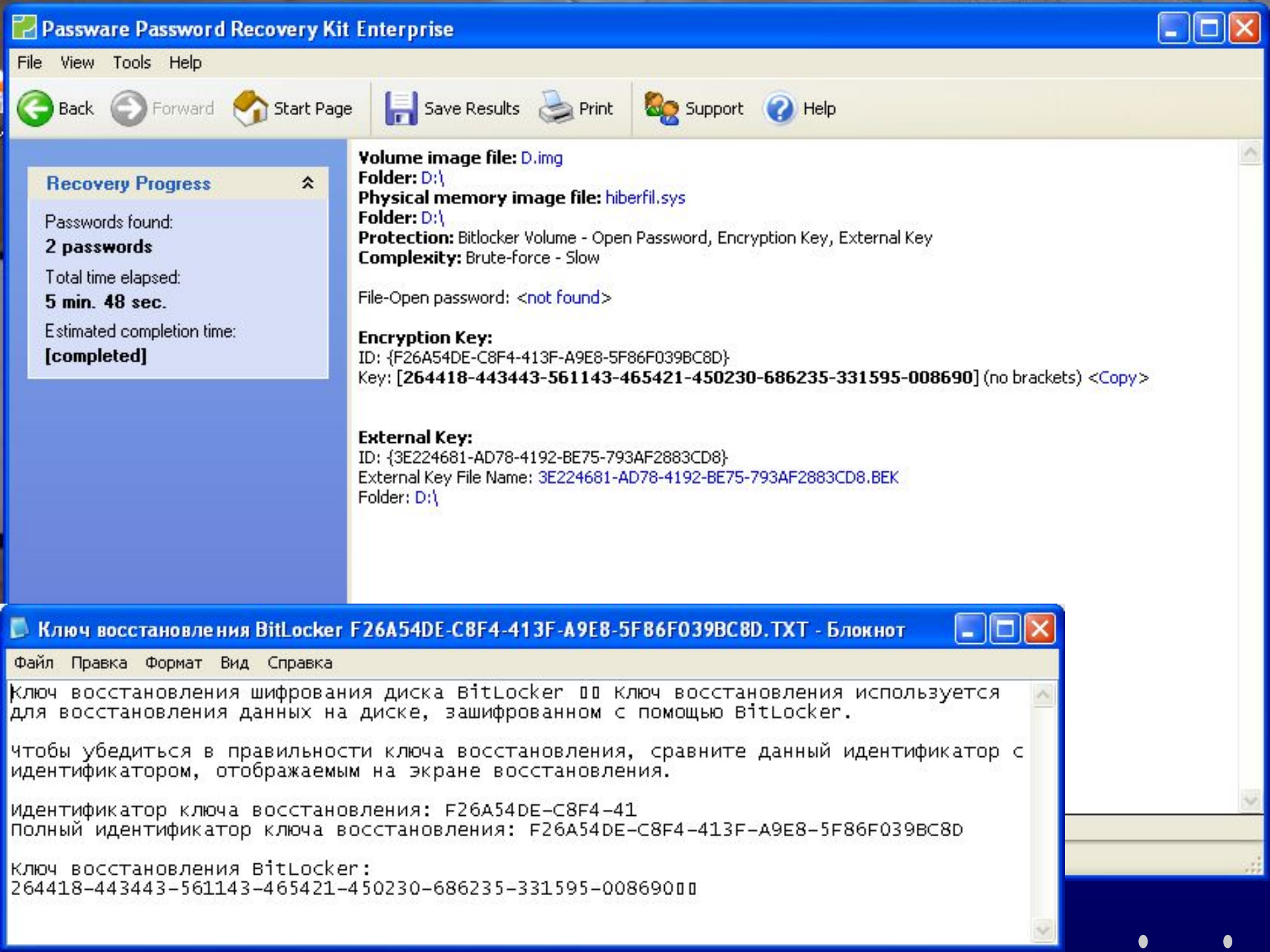

Шифрование диска BitLocker (D:)
Вставьте носитель с ключом восстановления и выберите этот диск
Выберите устройство, содержащее ключ восстановления
Съемный диск (F:)
Обновить
Поиск: Компьютер
й диск (D:)
вод (E:)
Ком... ▸ Съемн...
Поиск: Съемный диск (F:)
Упорядочить
Общий доступ
Новая папка
Имя
Дата изменения
Тип
3E224681-AD78-4192-BE75-793AF2883CD8.BEK
27.02.2012 21:06
Файл "BEK"
Локальный диск (D:) Состояни
Локальный диск

Атаки на BitLocker

- Атака при наличии файла гибернации
  - hiberfil.sys
- Атака полным перебором
  - 4 пароля/сек - 1 год для 4 символьного пароля


Passware Password Recovery Kit Enterprise
File View Tools Help
Back Forward Start Page Start Remove Move Down Move Up Sort by Duration Support Help
Actions
Display Tutorial
Attacks Wizard
Start Recovery
Remove All Attacks
Reset Attacks to Defaults
Save Attacks
Load Attacks
Details
Brute-force Attack checks all combinations of characters according to the current attack settings. This is the slowest, but most thorough, method.
D:\D.img
Protection: Bitlocker Volume - Open Password
Complexity: Brute-force - Slow
Change Casing Modifier: Lowercase
Complexity:
Passwords to check: 14 837 894 500 352
Brute-force Attack: Russian
Password Length: 6 to 7 characters
Complexity:
Symbol Set: Lower, Upper, Numbers
Passwords to check: 14 837 894 500 352
Add new attack here.
Drag attacks from this list:
Basic Attacks
Dictionary
Xieve
Brute-force
Known Password/Part
Previous Passwords
Modifiers
Change Casing
Reverse Password
Combine Attacks
Join Attacks
Append Attacks
Brute-Force Attack Settings
Minimum Length
Maximum Length
6
7
Language
Russian
Lowercase
Uppercase
Numbers
Advanced <<
Symbols
Space
Custom characters:
Pattern:
Start Recovery >>


Passware Password Recovery Kit Enterprise
File View Tools Help
Back Forward Start Page Support Help
Details
Passware Kit scans a memory image of a computer with a BitLocker or TrueCrypt encrypted volume and extracts all the encryption keys.
Select action from the list.
Hard Disk Encryption
BitLocker (Ctrl+B)
Recover encryption keys to unlock a BitLocker volume.
TrueCrypt (Ctrl+T)
Decrypt a TrueCrypt volume.


Passware Password Recovery Kit Enterprise
File View Tools Help
Back Forward Start Page Save Results Print Support Help
Recovery Progress
Passwords found:
2 passwords
Total time elapsed:
5 min. 48 sec.
Estimated completion time:
[completed]
Volume image file: D.img
Folder: D:\
Physical memory image file: hiberfil.sys
Folder: D:\
Protection: Bitlocker Volume - Open Password, Encryption Key, External Key
Complexity: Brute-force - Slow
File-Open password: <not found>
Encryption Key:
ID: {F26A54DE-C8F4-413F-A9E8-5F86F039BC8D}
Key: [264418-443443-561143-465421-450230-686235-331595-008690] (no brackets) <Copy>
External Key:
ID: {3E224681-AD78-4192-BE75-793AF2883CD8}
External Key File Name: 3E224681-AD78-4192-BE75-793AF2883CD8.BEK
Folder: D:\
Ключ восстановления BitLocker F26A54DE-C8F4-413F-A9E8-5F86F039BC8D.TXT - Блокнот
Файл Правка Формат Вид Справка
Ключ восстановления шифрования диска BitLocker ▯▯ Ключ восстановления используется для восстановления данных на диске, зашифрованном с помощью BitLocker.
Чтобы убедиться в правильности ключа восстановления, сравните данный идентификатор с идентификатором, отображаемым на экране восстановления.
Идентификатор ключа восстановления: F26A54DE-C8F4-41
Полный идентификатор ключа восстановления: F26A54DE-C8F4-413F-A9E8-5F86F039BC8D
Ключ восстановления BitLocker:
264418-443443-561143-465421-450230-686235-331595-008690▯▯

Ускорение

- Ускорение за счет использования вычислительной мощности GPU графических карт NVIDIA (пароля /сек)
  - MS BitLocker 4 92
  - RAR 3.x (AES) 315 5,000
  - MS Office 2010 (AES) 383 5,000
- Распределенное восстановление паролей


Passware Password Recovery Kit Enterprise
Distributed Password Recovery
Enable Distributed Password Recovery
Passware Kit Server port:
10777
Enable the built-in Passware Kit Agent
Hardware Acceleration
Enable nVidia GPU acceleration
OK
Cancel

Проверка целостности загрузочных компонентов до запуска ОС

- BIOS
- основной загрузочной записи (MBR)
- загрузочного сектора NTFS
- загрузочного блока NTFS
- диспетчера загрузки и управления доступом BitLocker

BitLocker To Go

- накопители с файловыми системами FAT, FAT32 и NTFS.
- AES с длиной ключа 128 (по умолчанию) или 256 бит
- пароль или смарт-карта