Фирма ИнфоКрипт

Инструкция по установке и эксплуатации WinNET 3.1

Назначение

ПО "WinNET 3.1" обеспечивает механизм усиленной аутентификации при входе в домен или локальный вход на сервер или рабочую станцию. Один из компонентов пароля хранится на носителе TouchMemory (в дальнейшем - TM), второй обязательный компонент является последовательностью символов уникальная для данного устройства TM. Другими возможными компонентами могут быть последовательность символов, вводимая с клавиатуры и последовательность символов уникальная для рабочей станции. Если при создании пароля используется компонента, вводимая с клавиатуры, то вход в домен только с TM без знания клавиатурной компоненты становится невозможным.

При создании пароля используется максимально возможная длина и комбинация 3-х из 4-х групп символов (1 –строчные буквы, 2 – прописные буквы, 3 – цифры, 4 – специальные символы), что значительно усложняет возможность его подбора какими-либо специальными средствами.

ПО "WinNET 3.1" обеспечивает удаленную аутентификацию пользователя по TM-паролю на сервере через

- Терминальную сессию MS Terminal Services.
- Терминальную сессию Citrix.

При этом на сервер не передается полное содержимое TM. Компонента пароля передается по безопасному зашифрованному соединению с проверкой подлинности удаленной стороны. Информация, передаваемая по каналу, шифруется с помощью алгоритма Диффи-Хеллмана. Реализация алгоритма Диффи-Хеллмана опирается *только* на функции программной библиотеки СКЗИ «Бикрипт», разработанной в фирме ИнфоКрипт.

ПО "WinNET 3.1" обеспечивает сетевой вход на разделяемые ресурсы доменов со считыванием пароля с носителя TM.

Системные требования

- ОС Windows 7, Windows Server 2008 R2/2012 R2
- Считыватель ключей:

  Плата СЗИ Аккорд-1 и выше или TM-считыватель Аккорд-RS; Драйвер TMDRV для Windows при использовании ключевого носителя TM.

Ключевые носители

Для хранения ключевой информации могут быть использованы носители типа TM. Носитель может содержать определенное количество учетных записей, принадлежащих как одному, так разным доменам, ограниченное только объемом памяти ключевого носителя.

Установка

Файл WinNet_S_3_1_x_x является инсталлятором ПО "WinNET 3.1", то есть программой выполняющей все необходимые действия по установке ПО "WinNET 3.1". Здесь x_x – версия WinNET 3.1

Инсталлятор предоставляет пользователю два варианта установки: обычный диалоговый вариант и установку из командной строки - так называемую "тихую установку".

Диалоговая установка

Для начала диалоговой установки пользователю достаточно вызвать от имени администратора инсталлятор WinNet-S_3_0_x_x.exe без параметров.

На экране появится приветствие мастера установки WinNET 3.1:

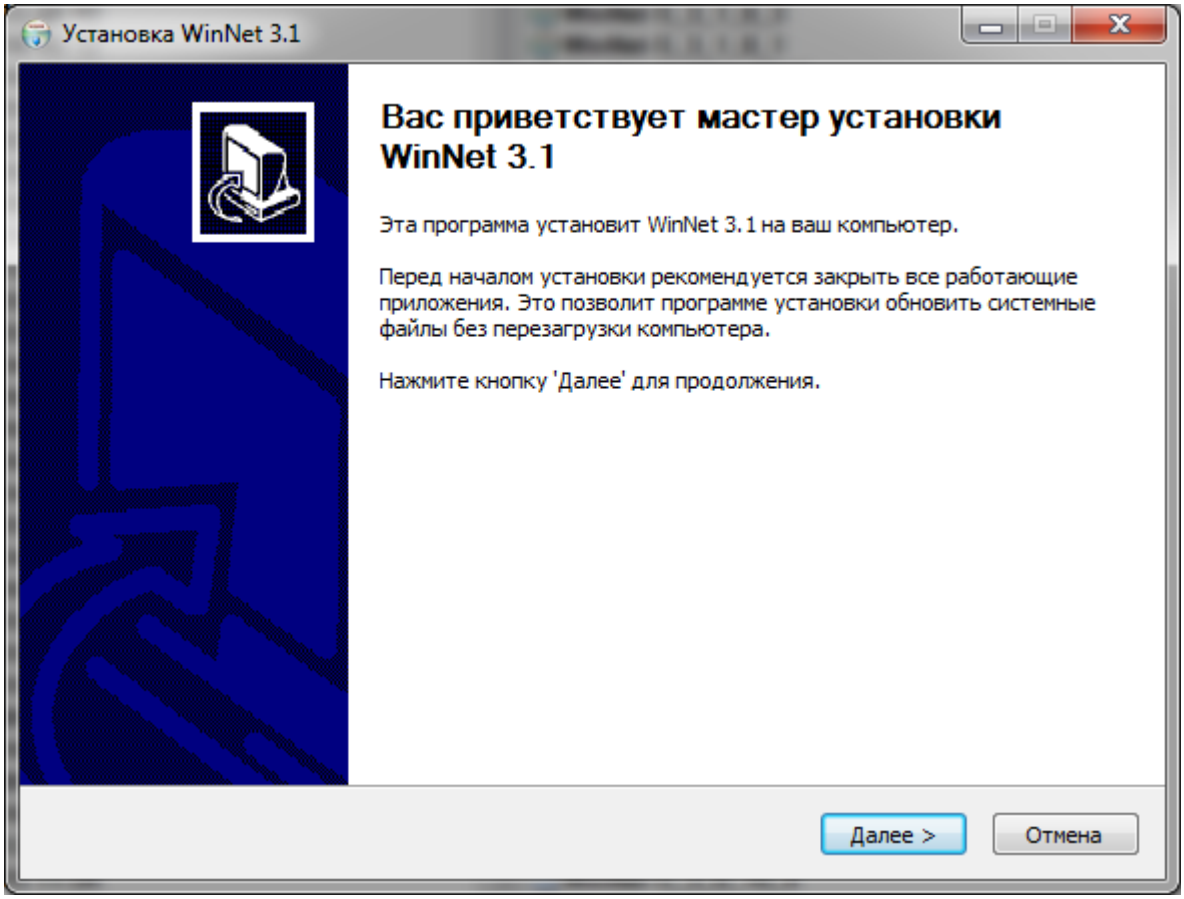


Рисунок 1. Приветствие мастера установки WinNET 3.1

Затем появится окно "Установка WinNET 3.1. Выбор папки установки".

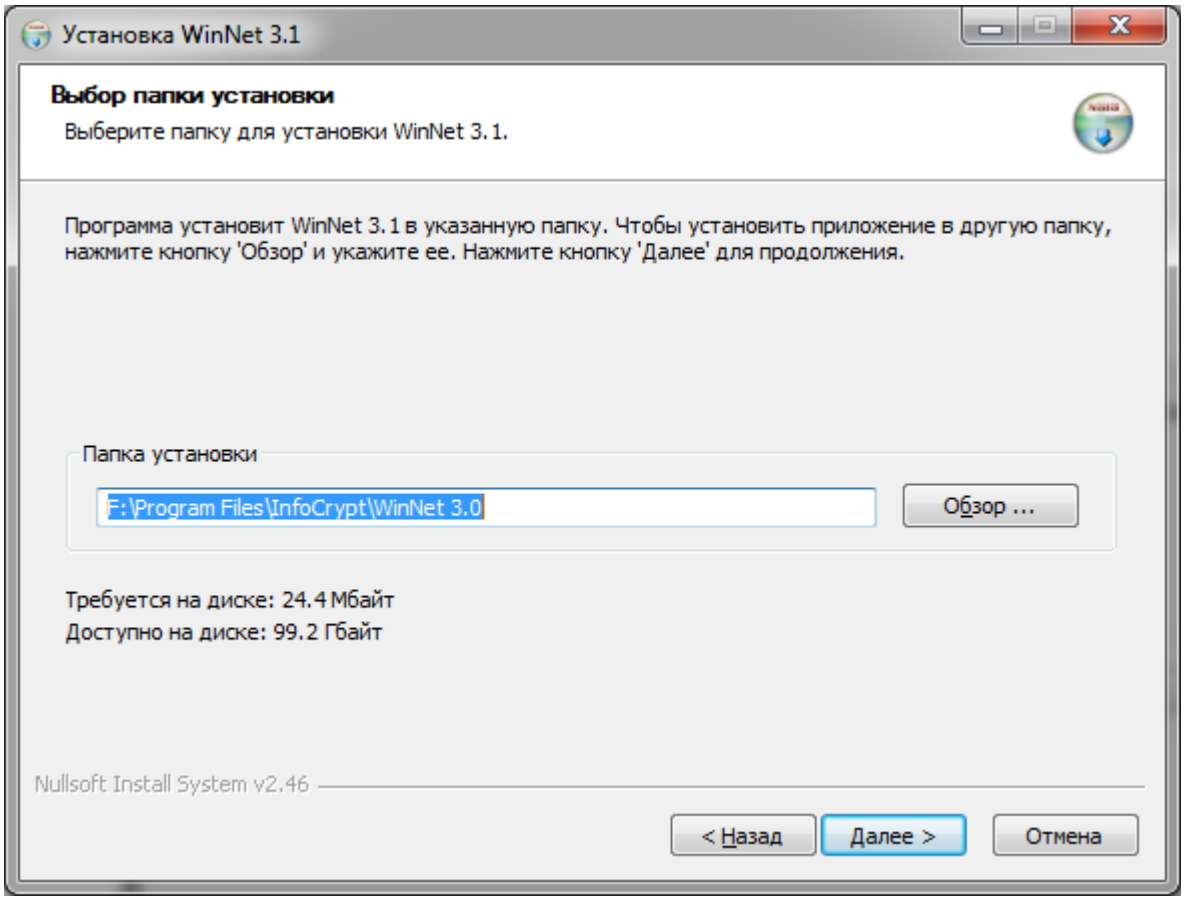


Рисунок 2. Выбор папки установки

С помощью этого окна пользователь может выбрать папку, куда будет выполнена установка ПО "WinNET 3.1".

После этого на экране монитора появится окно "Установка WinNET 3.1. Параметры установки":

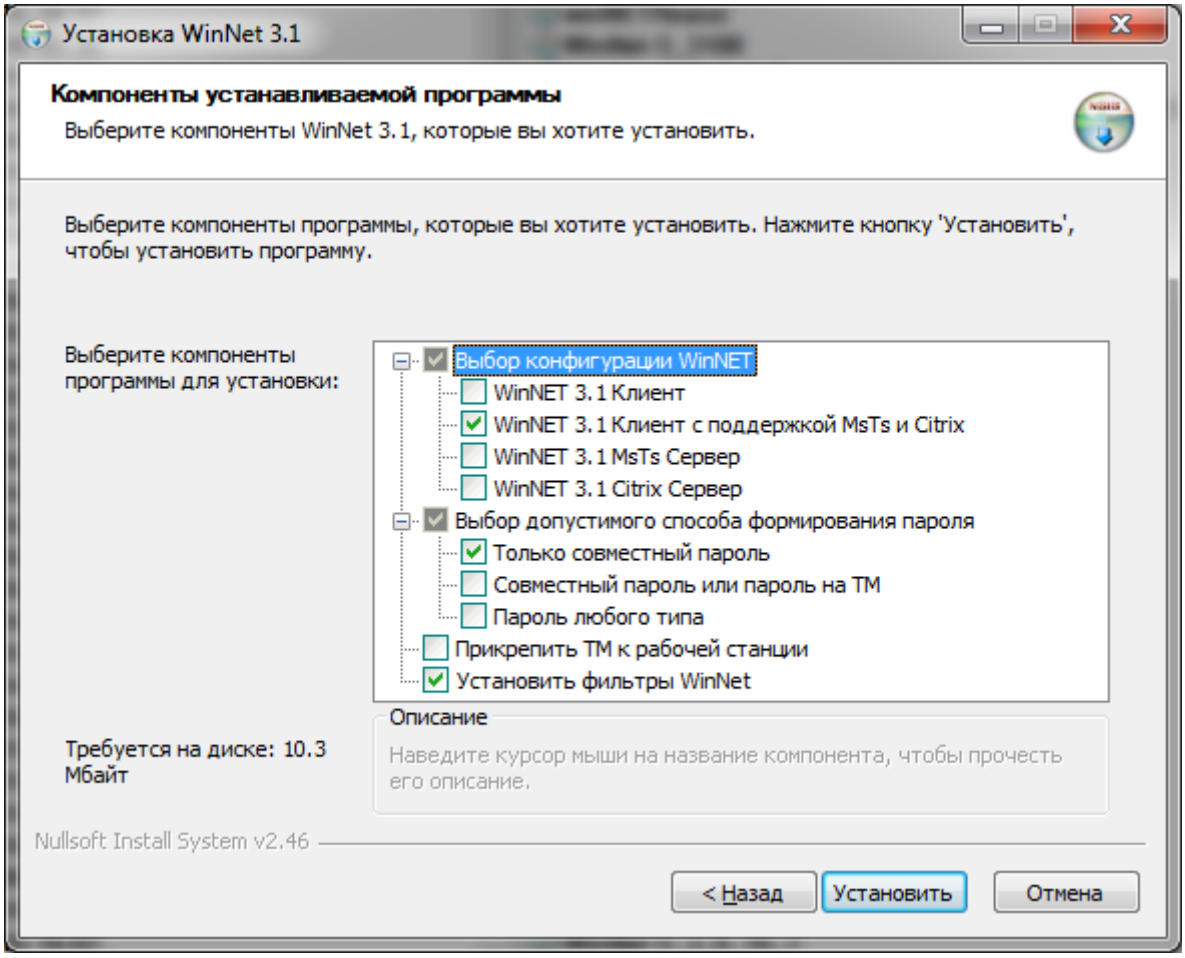


Рисунок 3. Установка ПО “WinNET 3.1”. Выбор параметров установки.

Первые четыре CheckBox дают возможность пользователю выбрать один из четырех возможных вариантов установки ПО “WinNET 3.1”:

WinNET 3.1 Клиент

Устанавливается только клиентская часть ПО “WinNET 3.1”.

WinNET 3.1 Клиент с поддержкой MsTs и Citrix

Устанавливается ПО “WinNET 3.1” и компоненты, позволяющие пользователю подключаться к удаленной рабочей станции через службу MS Terminal Services и через терминальную сессию Citrix так, что при авторизации происходит передача информации, считанной с ТМ на клиентском рабочем месте на стацию/сервер, к которой выполняется подключение. Такое подключение по MS TS возможно только к тем компьютерам, на которых установлен WinNET 3.1 MsTs Сервер. А подключение к виртуальным машинам Citrix возможно только к тем компьютерам, на которых установлен WinNET 3.1 Citrix Сервер.

Для работы с терминальными сессиями Citrix необходимо, чтобы на клиентской машине был установлен Citrix Receiver не старше 2012 года. При этом операционная система на клиентской машине должна быть 32-битной. Это обусловлено тем, что статическая библиотека vdapi.lib, необходимая для

разработки и функционирования виртуального Citrix-канала разработана компанией Citrix только в 32-битной версии.

WinNET 3.1 MsTs Сервер

устанавливается ПО “WinNET 3.1” и компоненты, позволяющие пользователю подключаться к данной рабочей станции через службу MS Terminal Services так, что при авторизации происходит передача информации, считанной с ТМ на удаленном рабочем месте на стацию/сервер, к которой выполняется подключение. Такое подключение возможно только с тех рабочих станций, на которых установлен WinNET 3.1 Клиент с поддержкой MsTs и Citrix.

WinNET 3.1 Citrix Сервер

устанавливается ПО “WinNET 3.1” и компоненты, позволяющие пользователю подключаться через терминальную сессию Citrix так, что при авторизации происходит передача информации, считанной с ТМ на удаленном рабочем месте на стацию/сервер, к которой выполняется подключение. Такое подключение возможно только с тех рабочих станций, на которых установлен WinNET 3.1 Клиент с поддержкой MsTs и Citrix.

Для успешной работы WinNet Citrix сервера на нем должен быть установлен пакет WF API для виртуальных каналов. Критическим является версия библиотеки wfapi.dll, которая не должна быть старше 2012 года. Ключевым является наличие в этой библиотеке функции WFGetActiveProtocol.

Следующие две опции позволяют ограничить пользователя, не входящего в группу Администраторы, в выборе способа формирования пароля.

Только совместный пароль

Пользователь при смене пароля может выбрать только пункт «Совместный пароль»

Совместный пароль или пароль на ТМ

Пользователь при смене пароля может выбрать один из пунктов «Совместный пароль» или «Пароль на ТМ»

Пароль любого типа

Пользователь, не имеющий административных прав, при смене пароля может выбрать любой пункт: «Совместный пароль», «Пароль на ТМ» или «Пароль любого типа».

Прикрепить ТМ к рабочей станции

В случае выбора этой опции при формировании пароля одной из компонент будет являться последовательность символов, уникальная для данной рабочей станции. При выборе этой опции вход в домен с помощью данной ТМ будет возможен только с данной рабочей станции.

Установить фильтры WinNet

В случае *не выбора* этой опции при установке WinNET 3.1 Citrix Сервер не будут установлены фильтры WinNetFilters. При всех остальных вариантах установки не выбрать эту опцию невозможно, а фильтры WinNetFilters устанавливаются.

При установке любой конфигурации ПО WinNET 3.1 в домашнюю директорию %PROGRAMFILES%\InfoCrypt\WinNet 3.1 будет помещена утилита clearPSWD с

помощью которой можно удалить с устройства ТМ все находящиеся на нем компоненты паролей ПО WinNET 3.1.

Затем появится окно, позволяющее отложить перезагрузку или немедленно ее выполнить.

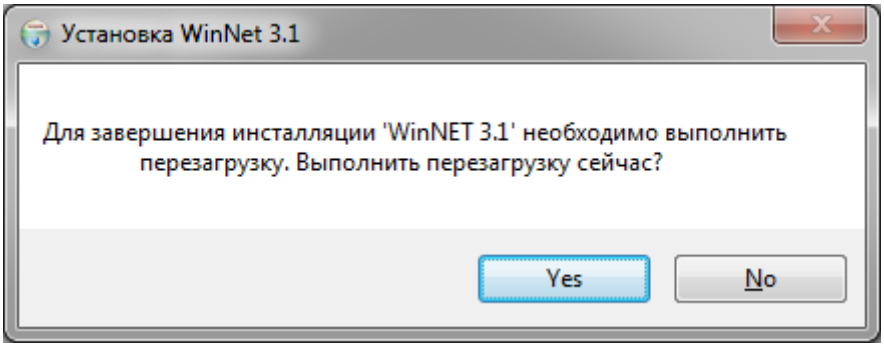


Рисунок 4. Установка ПО "WinNET 3.1". Сообщение о необходимости перезагрузить рабочую станцию.

Пакетная установка

Возможна инсталляция ПО "WinNET 3.1" в пакетном режиме, не требующая интерактивного ввода настроек. Для установки в данном режиме следует запустить инсталлятор с ключом командной строки "***/S***".

WinNet-S_3_0_x_x.exe /S

В этом случае установка ПО "WinNET 3.1" будет выполнена без дальнейшего участия пользователя в папку C:\Program Files\InfoCrypt\WinNet 3.0.

Прочие ключи командной строки:

/C - установка "WinNET 3.1 Клиент".

/Ms - установка "WinNET 3.1 MsTs Сервер".

/Ctx - установка "WinNET 3.1 Citrix Сервер".

/JT - совместный пароль или пароль на ТМ.

/AT - пароль любого типа, в том числе и клавиатурный.

/AW - прикрепить ТМ к рабочей станции.

/nF - не устанавливать фильтры WinNetFilters. Имеет смысл только совместно с опцией */Ctx*

/R - после завершения установки будет выполнена принудительная перезагрузка компьютера.

Опции по умолчанию:

- WinNET 3.1 Клиент с поддержкой MsTs и Citrix
- Только совместный пароль
- ТМ к рабочей станции не прикрепляется

- Перезагрузка не выполняется
- Фильтры WinNetFilter устанавливаются

Изменения после установки

В случае успешной установки на рабочей станции происходят изменения, зависящие от выбранного варианта установки.

WinNET 3.1 Клиент

В Control Panel -> Programs and Features ПО "WinNet 3.1" отображается как "InfoCrypt WinNET 3.1 Client ".

- В папке %PROGRAMFILES% будет создана папка InfoCrypt\WinNET 3.0, в которую будет помещены данный документ и следующие файлы:
  - InfoCryptAdmin.pdf - описание ActiveX компонента InfocryptAdmin.dll, позволяющего аутентифицироваться в приложениях с помощью ТМ.
  - InfoCryptAdminSampleNew.html - пример использования InfocryptAdmin.dll, написанный на JavaScript.
  - accnetsb.lib - lib-файл к библиотеке accnetsb.dll.
  - WinNetDevice.lib - lib-файл к библиотеке WinNetDevice.dll.
  - bicr_adm.dll, grn.dll - модули программной библиотеки СКЗИ «Бикрипт».
  - ClearPSWD.exe - утилита, стирающая все пароли на приложенном устройстве ТМ.
  - MigratePswd.exe - утилита, позволяющая выполнить в полуавтоматическом режиме миграцию компонент паролей из одного домена в другой.
  - CheckPswd.exe - утилита, позволяющая определять есть ли на приложенном устройстве ТМ компоненты пароля из заданного списка пар <UserName,DomainName>
  - WinNetUninstall.exe - модуль, выполняющий деинсталляцию WinNet 3.1
- В папке %WINDIR%\System32 на x86 (%WINDIR%\SysWOW64 на x64) появятся модули:
  - InfocryptAdmin.dll - ActiveX компонента InfocryptAdmin.dll, позволяющего аутентифицироваться в приложениях с помощью ТМ.
  - accnetsb.dll, random.dll - библиотеки, необходимые для работы InfocryptAdmin.dll.
- В папке %WINDIR%\System32 на x86 (%WINDIR% на x64) появятся модули:
  - WinNetProvider.dll - регистрируется как дополнительный провайдер, обеспечивающий аутентификацию пользователя с помощью ТМ, в частности в ветке реестра

HKLM\SOFTWARE\Microsoft\CurrentVersion\Authentication\Credential Providers появится папка {D265960-….}, содержащая единственную запись:
(Default) WinNetProvider

- WinNetTrapper.exe - обеспечивает ввод пароля с устройства считывания при запуске некоторых приложений. WinNetTrapper.exe вносится в список пользовательских приложений, стартующих при входе пользователя в систему: в ветке реестра HKLM SOFTWARE\Microsoft\Windows\CurrentVersion\Run появляется соответствующая запись.
- WinNetTrapper.dll - библиотека, необходимая для работы модуля WinNetTrapper.exe
- WinNetFilter.dll - дополнительный фильтр, обеспечивающий блокировку tiles, которые выводятся на экран самой операционной системой. В ветке реестра

  HKLM\SOFTWARE\Microsoft\CurrentVersion\Authentication\Credential Providers Filters

  появится папка {C7A4083C-….}, содержащей единственную запись:

  (Default) WinNetFilter
- WinNetDevice.dll - библиотека для работы с устройством ТМ.

- В ветке реестра

  HKLM SOFTWARE\\InfoCrypt\\WinNet 3.1 появятся записи

  InstallDir %PROGRAMFILES%\InfoCrypt\WinNet 3.0

  HomePath %PROGRAMFILES%\InfoCrypt\WinNet 3.0

  и некоторые другие.

WinNET 3.1 Клиент с поддержкой MsTs и Citrix

В этом случае устанавливается "WinNET 3.1 Клиент", выполняются все изменения, связанные с его установкой. В Control Panel -> Programs and Features ПО "WinNet 3.1" отображается как "InfoCrypt WinNET 3.1 Client Citrix MsTs ". Дополнительно:

1. В домашней папке %PROGRAMFILES%\InfoCrypt\WinNet 3.0 появятся файлы bicr_adm64.dll и grn64.dll - 64-битный версии программной библиотеки СКЗИ «Бикрипт».

2. Устанавливается MS TS клиент.

- В папке %WINDIR% появится модуль rdp_client_winnet.dll
- rdp_client_winnet.dll регистрируется как модуль расширения MS Terminal Services: в ветке реестра

  HKCU Software\Microsoft\Terminal Server Client\Default\AddIns\SamuraiClient

  появляется запись

  Name %WINDIR%\rdp_client_winnet.dll

3. Устанавливается Citrix клиент, но только на платформе x86. Это обусловлено тем, что статическая библиотека vdapi.lib, необходимая для разработки и функционирования виртуального Citrix-канала разработана компанией Citrix только в 32-битной версии.

- В папке %PROGRAMFILES%\Citrix\ICA Client появится модуль ctx_client_winnet.dll
- Модуль ctx_client_winnet.dll будет зарегистрирован как модуль расширения ICA Client. Будет создана ветка реестра

HKLM SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\WinNetCitrixClient

В этой ветке появятся три записи:

DriverName	Unsupported
DriverName16	Unsupported
DriverName32	ctx_client_winnet.dll

А в ветке реестра

HKLM "SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\ICA 3.0

запись

VirtualDriverEx <Список расширений ICA клиента>

превратится в

VirtualDriverEx <Список расширений ICA клиента>,WinNetCitrixClient

WinNET 3.1 MsTs Сервер

В этом случае устанавливается "WinNET 3.1 Клиент" и выполняются все изменения, связанные с его установкой. В Control Panel -> Programs and Features ПО "WinNet 3.1" отображается как "InfoCrypt WinNET 3.1 MsTs Server".

WinNET 3.1 Citrix Сервер

В этом случае устанавливается "WinNET 3.1 Клиент" и выполняются все изменения, связанные с его установкой. В Control Panel -> Programs and Features ПО "WinNet 3.1" отображается как "InfoCrypt WinNET 3.1 Citrix Server".

Утилиты

Независимо от выбранного варианта установки в домашнюю папку WinNET 3.1 будут записаны три утилиты.

- checkPswd - утилита, позволяющая определять есть ли на приложенном устройстве ТМ компоненты пароля из заданного списка пар <UserName,DomainName>. Аргументы командной строки:

  checkPswd.exe UserDomainList,

  где UserDomainList файл, содержащий список пар <UserName,DomainName> разделенных запятой, по одной паре в строке:

  User1,Domain1

  User2,Domain2

  . . .

- clearPSWD - утилита, стирающая все пароли на приложенном устройстве ТМ. Эта утилита запускается без аргументов.

- migratePswd - утилита, позволяющая выполнить в полуавтоматическом режиме миграцию компонент паролей из одного домена в другой. Сама компонента пароля при этом не изменяется, изменяется домен и, возможно, логин пользователя. Аргументы командной строки:

  migratePswd.exe oldDomain newDomain userListFile
  где:

  oldDomain - имя домена, компоненты паролей для которого находятся на устройстве ТМ. Это - имя "старого" домена *откуда* мигрируем.

  newDomain - имя домена, компоненты паролей для которого будут записаны на устройство. Это - имя "нового" домена *куда* мигрируем.

  userListFile - содержащий список пар <UserOldName,UserNewName> разделенных запятой, по одной паре в строке. UserOldName - имя пользователя в "старом" домене, UserNewName - имя пользователя в "новом" домене

Log-файл

ПО "WinNET 3.1" может протоколировать критические операции, записывая их в log-файл с именем %PROGRAMFILES%\InfoCrypt\WinNET_30.txt.

Для того чтобы активировать протоколирование необходимо в ветку реестра

HKLM SOFTWARE\InfoCrypt\WinNET 3.0

Добавить запись

LogFile Yes

Если в эту же ветку реестра добавить запись

LogFileSize X

То размер записываемого log-файла будет ограничен X мегабайтами

Примечание. Рекомендуемым режимом является режим без протоколирования. При обнаружении ошибок следует включить режим протоколирования, воспроизвести ситуацию, приводящую к ошибке и отослать log-файл А.М.Дьякову AMDyakov@sberbank.ru (или непосредственно разработчикам: В.К.Николаеву V.Nikolaev@InfoCrypt.ru).

Это может существенно сократить время, необходимое для исправления ошибки.

Исключительные ситуации

В процессе установки могут возникнуть исключительные ситуации, при которых установка ПО "WinNET 3.1" или некоторых его компонент не может быть выполнена корректно. Это может быть, например, следствием попытки установить ПО "WinNET 3.1" не от имени администратора рабочей станции или попытки установить ПО "WinNET 3.1" на станцию, на которой с помощью групповых политик Active Directory ресурсы, которые необходимо модифицировать в процессе установки, защищены от модификации и т.д.

В таком случае:

- при диалоговой установке на экране будут появляться предупреждения, в которых указываются этапы установки, которые не удается выполнить.
- при "тихой" установке в папке, из которой выполнялся запуск инсталлятора, будет создан файл WinNet_30.txt, в котором будут перечислены все не выполненные этапы установки.

Эксплуатация

После установки ПО "WinNET 3.1" на рабочей станции произойдут следующие изменения.

Окно входа в Windows

Изменится внешний вид окна входа в Windows - каждый пользовательский tile будет снабжен в нижней его части подписью WinNET 3.1. Рисунок 5а показывает изменения в случае, когда рабочая станция включена в рабочую группу, Рисунок 5в – в случае, когда рабочая станция включена в домен.

Рисунок 5а. Состояние окна входа в Windows 7, в случае, когда рабочая станция включена в рабочую группу.

A) До установки ПО "WinNET 3.1"

B) Непосредственно после установки " WinNET 3.1"

После установки " WinNET 3.1" отображаются tiles тех и только тех пользователей, которые отображались до установки "Аккорд WinNET 3.1". При этом все пользователи сохранили свои tiles, но каждый tile получил в нижней его части подпись WinNET 3.1.

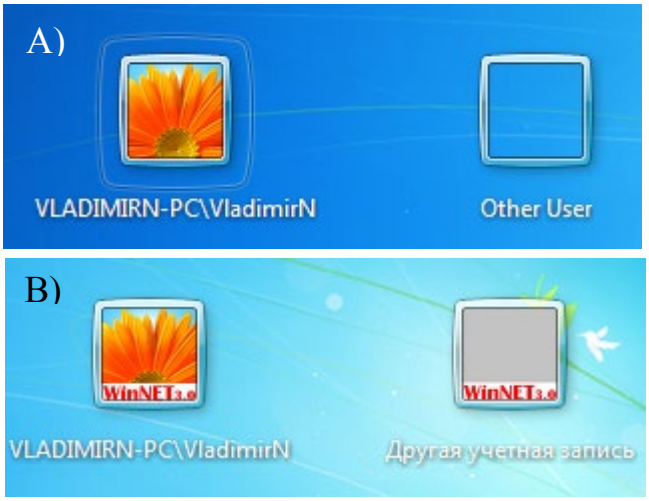


Рисунок 5в. Состояние окна входа в Windows 7 в случае, когда рабочая станция включена в домен.

A) До установки ПО "Аккорд WinNET 3.1"

B) После установки ПО "Аккорд WinNET 3.1".

Отметим, что, если пользователь при установленном ПО "WinNET 3.1" поменяет свой tile, то именно этот вновь выбранный tile будет отображаться в окне входа в Windows. Если пользователь будет удален, то его tile перестанет отображаться в окне входа. Если будет создан новый пользователь, то соответствующий tile появится в окне входа в Windows.

На Рисунке 5в видно, что, несмотря на то, что ПО "WinNET 3.1" устанавливался на англоязычную версию Windows, после его установки произошла частичная русификация, касающаяся диалогов, связанных с входом в Windows.

Вход в Windows

После установки ПО "WinNET 3.1" при входе в Windows, после выбора и активизации пользовательского tile, к обычным элементам диалога входа добавляется ComboBox – Рисунок 6.

A 

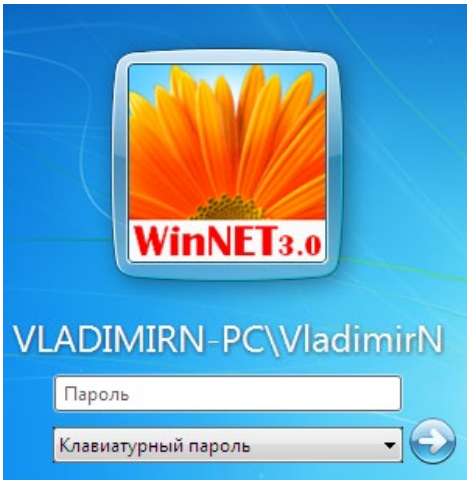
B 

Рисунок 6. Активированный tile пользователя VladimirN.
A) До установки ПО "Аккорд WinNET 3.1"
B) После установки "Аккорд WinNET 3.1"

С помощью этого ComboBox пользователь может выбрать один из трех возможных способов формирования пароля:

- Клавиатурный пароль – обычный клавиатурный пароль;
- Пароль на ТМ – формируемый пароль, содержит компоненту, хранящуюся на устройстве считывания TouchMemory;
- Совместный пароль – пароль, формируемый из части, вводимой с клавиатуры, и части, хранящейся на ТМ.

Чаще всего, при первом входе в Windows, после установки ПО "WinNET 3.1", пользователь выберет "Клавиатурный пароль" (то есть обычный клавиатурный пароль). Однако существуют ситуации, когда необходимы и другие возможности, например, после переустановки ПО "WinNET 3.1", а также при входе пользователя в домен, если этот пользователь на другой рабочей станции уже изменил свой способ формирования пароля.

Если пользователь с помощью диалога "Сменить пароль" изменит и способ формирования пароля, то при следующем входе в этом ComboBox будет выбран соответствующий способ формирования пароля – Рисунок 7.

Рисунок 7. Возможные состояния диалога входа на рабочую станцию в зависимости от выбранного способа формирования пароля. Пользователь Pele использует обычный клавиатурный пароль (он выбрал “Клавиатурный пароль”), пользователь Chigorin использует устройство считывания ТМ (он выбрал “Пароль на ТМ”), а пользователь Lennon – комбинированный метод, при котором одна часть пароля хранится на ТМ, а вторая вводится с клавиатуры – он выбрал “Совместный пароль”.

Если пользователь выбрал способ формирования пароля, использующий устройство считывания ("Пароль на ТМ" или "Совместный пароль"), то после нажатия на  на экране появится приглашение приложить устройство считывания - Рисунок 8. Пользователь должен в течение примерно одной минуты приложить устройство считывания к считывающему устройству.

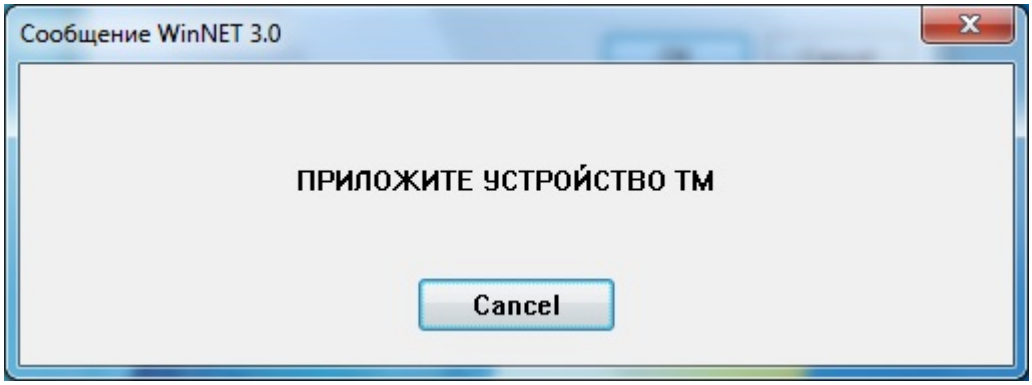


Рисунок 8. Приглашение приложить устройство ТМ для чтения пароля

Если пароль был обнаружен и успешно считан, на экране появится соответствующее сообщение – Рисунок 9. Пользователю не требуется ничего делать – через две секунды это сообщение само исчезнет с экрана.

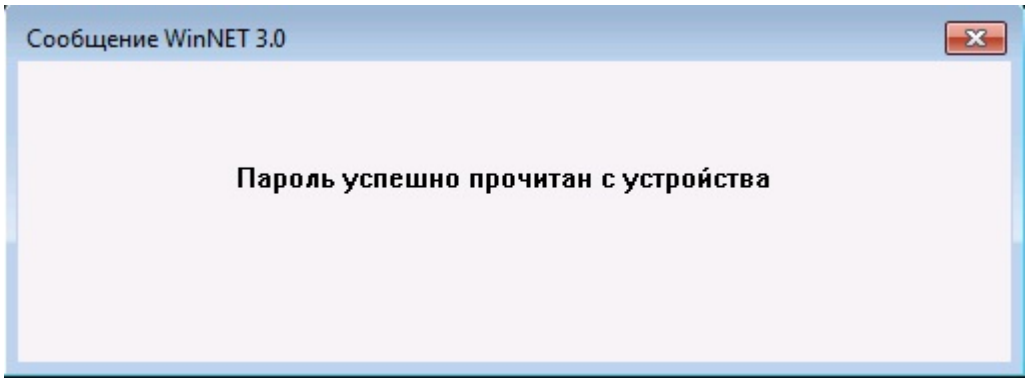


Рисунок 9. Сообщение об успешном считывании пароля с устройства ТМ

Если же в процессе считывания была встречена какая-либо ошибка, то на экране появится сообщение, в котором указывается причина невозможности считывания пароля и ее код.

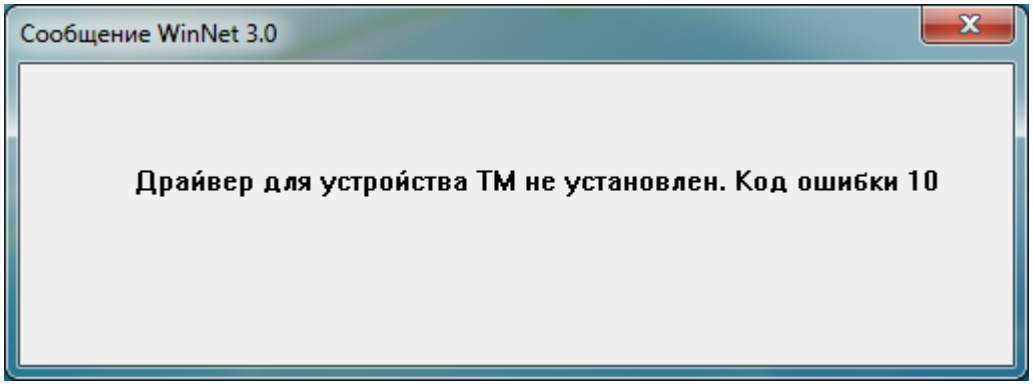


Рисунок 10. Сообщение WinNET 3.1 об отсутствии драйвера, необходимого для работы с устройством ТМ.

На Рисунке 10 приведен пример сообщения, когда считывания пароля с устройства невозможно, поскольку на компьютере не установлен драйвер устройства ТМ.

Смена пароля

После установки ПО "WinNET 3.1" изменяется и диалог "Смена пароля". В этом случае к обычным элементам диалога добавляется два ComboBox – один, для задания способа формирования старого пароля, а второй – для выбора пользователем способа формирования нового пароля - Рисунок 11.

A)

B)

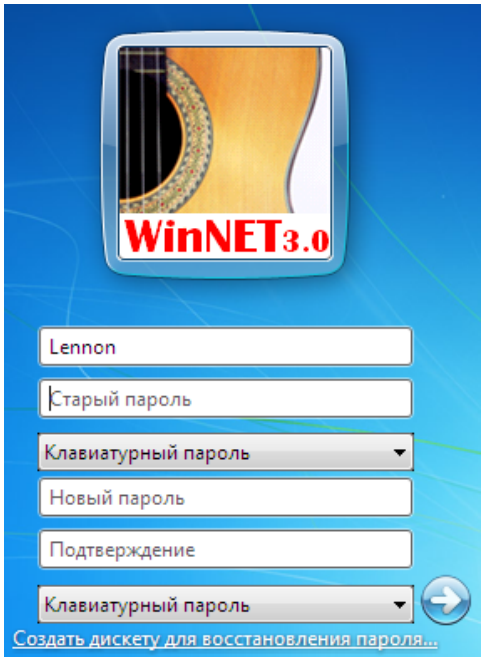


Рисунок 11. Диалог смены пароля.
A) До установки ПО "Аккорд WinNET 3.1"
B) После установки "Аккорд WinNET 3.1".

На рисунке 12 приведены примеры смен пароля для различных ситуаций. Для пользователя, имеющего права Администратора допустимы все 9 переходов. Обычный пользователь может сменить пароль или только на "Совместный пароль" или на "Пароль на ТМ" или "Совместный пароль" выбор делается при установке "WinNET 3.1".

Рисунок 12. Примеры смены пароля.
Пользователь Pele, текущий пароль которого является клавиатурным паролем, готов сменить его на "Пароль на ТМ". Пользователь Chigorin, текущий пароль которого является "Пароль на ТМ", собирается сменить пароль, а в качестве способа его формирования выбрал "Совместный пароль". Пользователь Lennon, использовавший "Совместный пароль", готовится сменить его на обычный клавиатурный пароль.

При смене пароля в случаях, когда выбранный способ хранения создаваемого пароля требует прикладывания устройства считывания, на экране появится приглашение – Рисунок 8. Как и при чтении пароля у пользователя есть примерно одна минута для того, чтобы найти и приложить устройство.

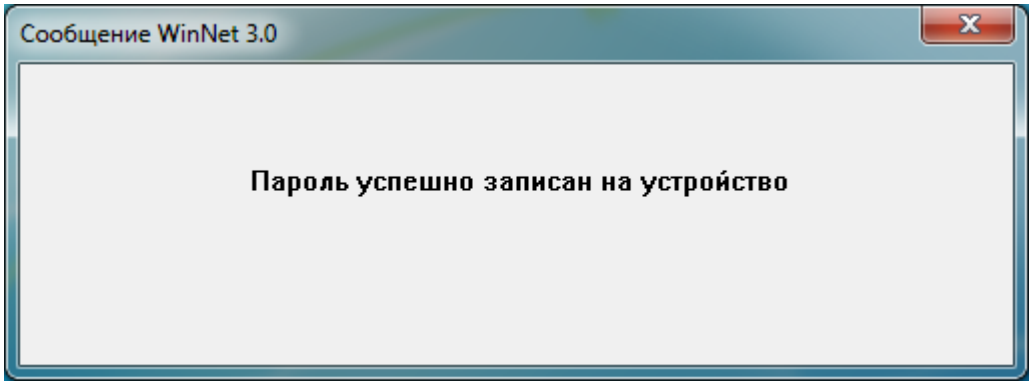


Рисунок 13. Сообщение об успешной записи пароля на устройство.

При успешной записи пароля на устройство на экране появится соответствующее сообщение – Рисунок 13. Пользователю не требуется ничего делать – через две секунды это сообщение само исчезнет с экрана.

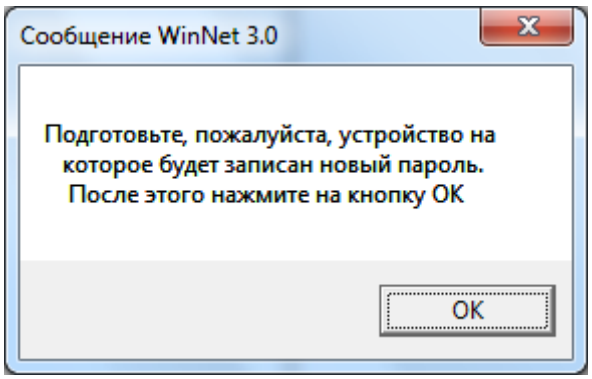


Рисунок 14. Сообщение ПО "Аккорд WinNET 3.1" о необходимости подготовить устройство для записи нового пароля.

При смене пароля в случаях, когда и существующий и выбранный способы хранения пароля требуют прикладывания устройства считывания, после того, как пользователь приложит устройство для *считывания* существующего пароля и перед тем, как появится приглашение приложить устройство для *записи* нового пароля, для удобства пользователя на экране появляется сообщение, показанное на рисунке 14.

Особые случаи, возникающие при смене пароля

Как и при чтении пароля при смене пароля в случае возникновения ошибки на экран будет выведено сообщение, в котором приводится причина ошибки и ее код.

Существует два особых случая.

Переполнение устройства.

В процессе смены пароля выясняется, что для записи нового пароля на устройстве ТМ нет свободного места. В таком случае на экране появляется следующее сообщение:

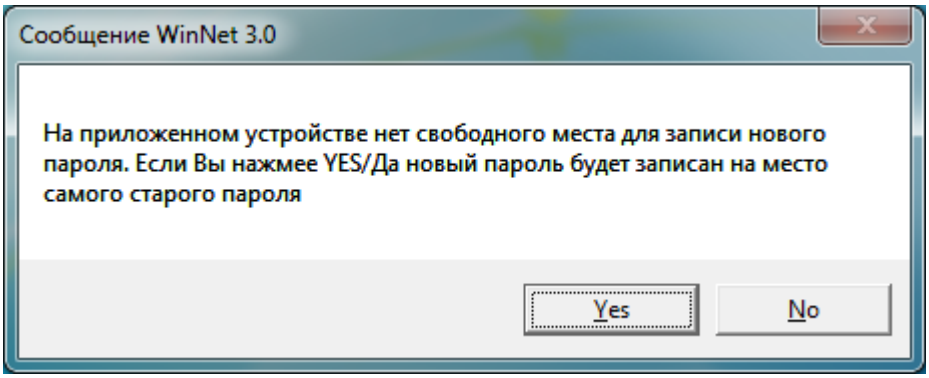


Рисунок 15. Сообщение в случае отсутствия свободного места на устройстве

Если пользователь выберет No/Нет, то процесс записи пароля на ТМ и смены пароля будет остановлен - у пользователя останется старый пароль.

Если пользователь выберет Yes/Да, то новый пароль будет записан на место самого старого. Слова "самый старый" надо понимать в следующем смысле. Пароли записываются на устройство в определенном порядке: первый, второй, третий и т.д. Самым старым паролем называется пароль, который в этом порядке является первым.

Невозможность смены пароля.

В условиях действия запретительной парольной политики попытка сменить пароль будет блокирована. При этом на экране появится сообщение - Рисунок 16. Если действующий пароль был паролем на ТМ, то компонента пароля, хранящаяся на ТМ не будет испорчена и старый "Пароль на ТМ" будет сохранен.

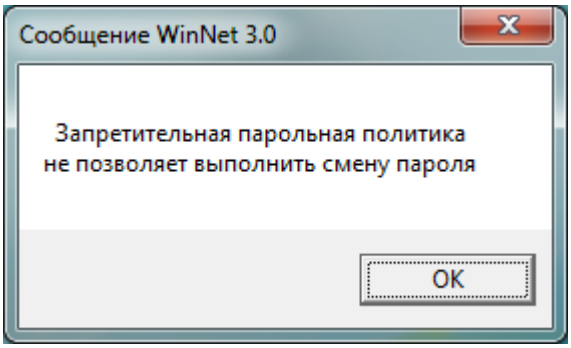


Рисунок 16. Сообщение о невозможности сменить пароль.

Другие сценарии аутентификации

Существуют ситуации, когда пользователю требуется выполнить операцию, для которой у него нет прав. В таких случаях на экране появляется диалог, требующий ввода учетной записи и пароля пользователя обладающего достаточными правами для выполнения требующейся операции. После установки ПО "WinNET 3.1" эти диалоги появляются в, так сказать, WinNET виде: tile снабжен надписью WinNET 3.1 и кроме обычных элементов диалога присутствует ComboBox, позволяющий выбрать способ формирования пароля.

Приведем несколько таких сценариев.

Включение рабочей станции в домен

При включении рабочей станции в домен появится следующий диалог (Рисунок 17), в котором следует ввести учетную запись и пароль администратора домена, в который включается компьютер.

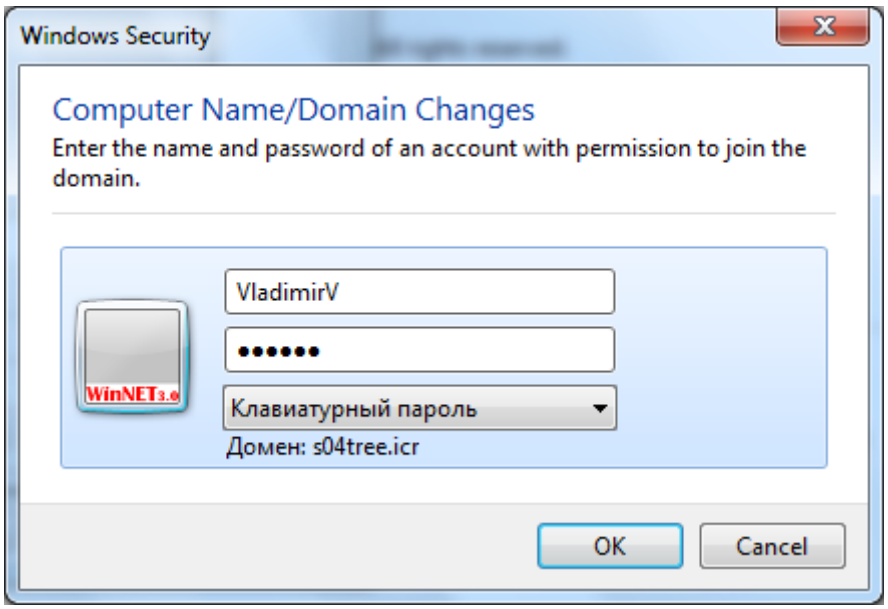


Рисунок 17. Диалог включения рабочей станции в домен.

Включение рабочей станции в рабочую группу – исключение из домена

Если пользователь, не являющийся администратором рабочей станции, попытается исключить компьютер из домена и включить его в рабочую группу, то для этого ему потребуется ввести учетную запись и пароль администратора рабочей станции с помощью следующего диалога – Рисунок 18.

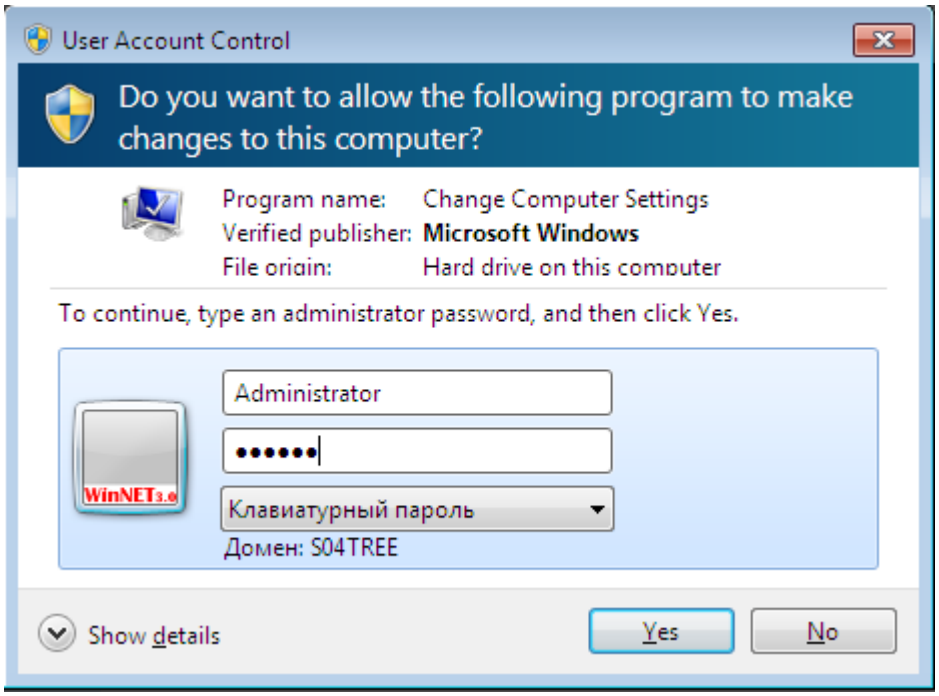


Рисунок 18. Диалог, появляющийся при исключении рабочей станции из домена и включении ее в рабочую группу.

Подключение сетевого ресурса

Если пользователь попытается подключить сетевой ресурс, на подключение которого у него нет прав, на экране появится следующий диалог – Рисунок 19.

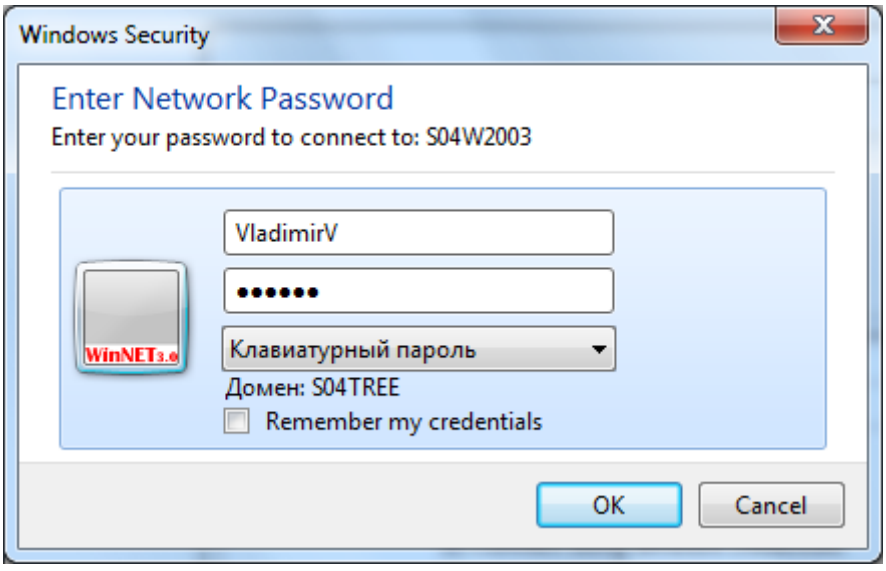


Рисунок 19. Диалог для ввода сетевого пароля при подключении сетевого или доменного ресурса.

Совместимость с ПО "WinNET 1.0"

Данная версия совместима с ПО "Аккорд WinNET 1.0". Точнее: пароли, записанные на носители с помощью ПО "Аккорд WinNET 1.0", корректно зачитываются и обрабатываются с помощью ПО "WinNET 3.1". Однако, если на носитель, хранящий пароль в формате ПО "Аккорд WinNET 1.0", будет записан пароль с помощью ПО "WinNET 3.1", то пароль формата ПО "Аккорд WinNET 1.0" будет утрачен. [1)]

При входе в компьютер (или домен) с помощью устройства, на котором записан пароль в формате ПО "Аккорд WinNET 1.0", вместо сообщения о благополучном считывании пароля с устройства (Рисунок 9) на экран монитора выдается предупреждение, показанное на Рисунке 20.

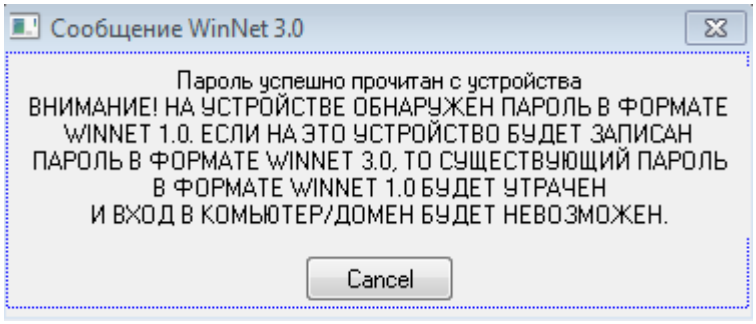


Рисунок 20. Сообщение о том, что на приложенном устройстве обнаружен пароль в формате ПО "Аккорд WinNET 1.0".

Особые ситуации при тестировании

Теоретически в процессе тестирования возможна ситуация, когда нет возможности штатными средствами снять ПО "WinNET 3.1" и вообще нет возможности войти на рабочую станцию. В настоящий момент выйти из такой ситуации можно следующим образом: зайти на станцию в Safe-моде, удалить записи в реестре, регистрирующие WinNetProvider.dll как дополнительного провайдера и WinNetFilter.dll как дополнительный фильтр и удалить сами эти файлы из папки C:\Windows\System32.

- Динамически загружаемая библиотека WinNetProvider.dll, зарегистрирована как дополнительный провайдер, обеспечивающий вход в Windows 7: в ветке реестра

  HKLM\SOFTWARE\Microsoft\CurrentVersion\Authentication\Credential Providers

  присутствует папка {D265960-….}, содержащая единственную запись:

  (Default) WinNetProvider

- Динамически загружаемая библиотека WinNetFilter.dll зарегистрирована как дополнительный фильтр, обеспечивающий фильтрацию tiles, которые выводятся на экран самой операционной системой: в ветке

  HKLM\SOFTWARE\Microsoft\CurrentVersion\Authentication\Credential Providers Filters

  присутствует папка {C7A4083C-….}, содержащая единственную запись:

  (Default) WinNetFilter

Для того чтобы снять компонент WinNetTrapper.exe, автоматически стартующий при загрузке, достаточно

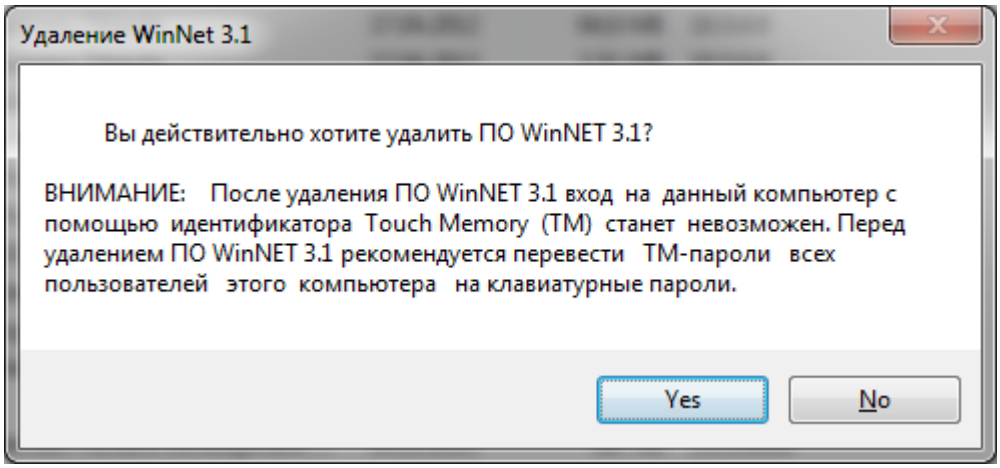
- удалить процесс WinNetTrapper;

[1)] Начиная с версии 3.0.2 в таком случае существовавший пароль в формате Аккорд WinNET 1.0 физически стирается с устройства.

- в ветке реестра HKLM SOFTWARE\Microsoft\Windows\CurrentVersion\Run удалить запись с ключом WinNetTrapper;
- перезагрузить рабочую станцию.

Удаление ПО “WinNET 3.1”

Удаление ПО "WinNET 3.1" выполняется как обычно через Панель управления → Программы → Программы и Компоненты → Удаление Программ. Можно непосредственно выполнить программу WinNetUninstall.exe, находящуюся в папке C:\Program Files\InfoCrypt.



При запуске этой программы на экране появится предупреждение – Рисунок 21. Если после ознакомления с этим предупреждением у пользователя не исчезнет желание удалить ПО "WinNET 3.1", то ему следует кликнуть на кнопку "Да/Yes" и процесс снятия ПО "WinNET 3.1" стартует.

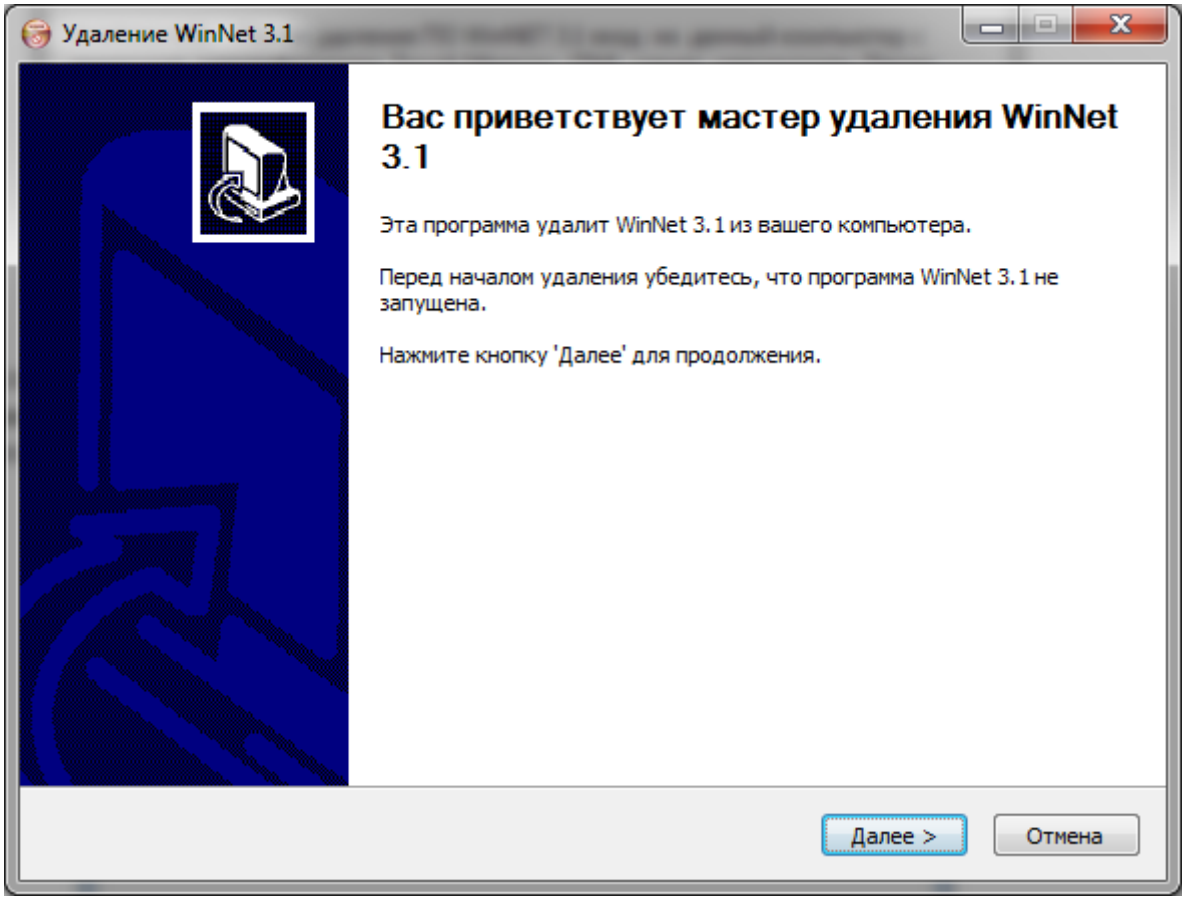
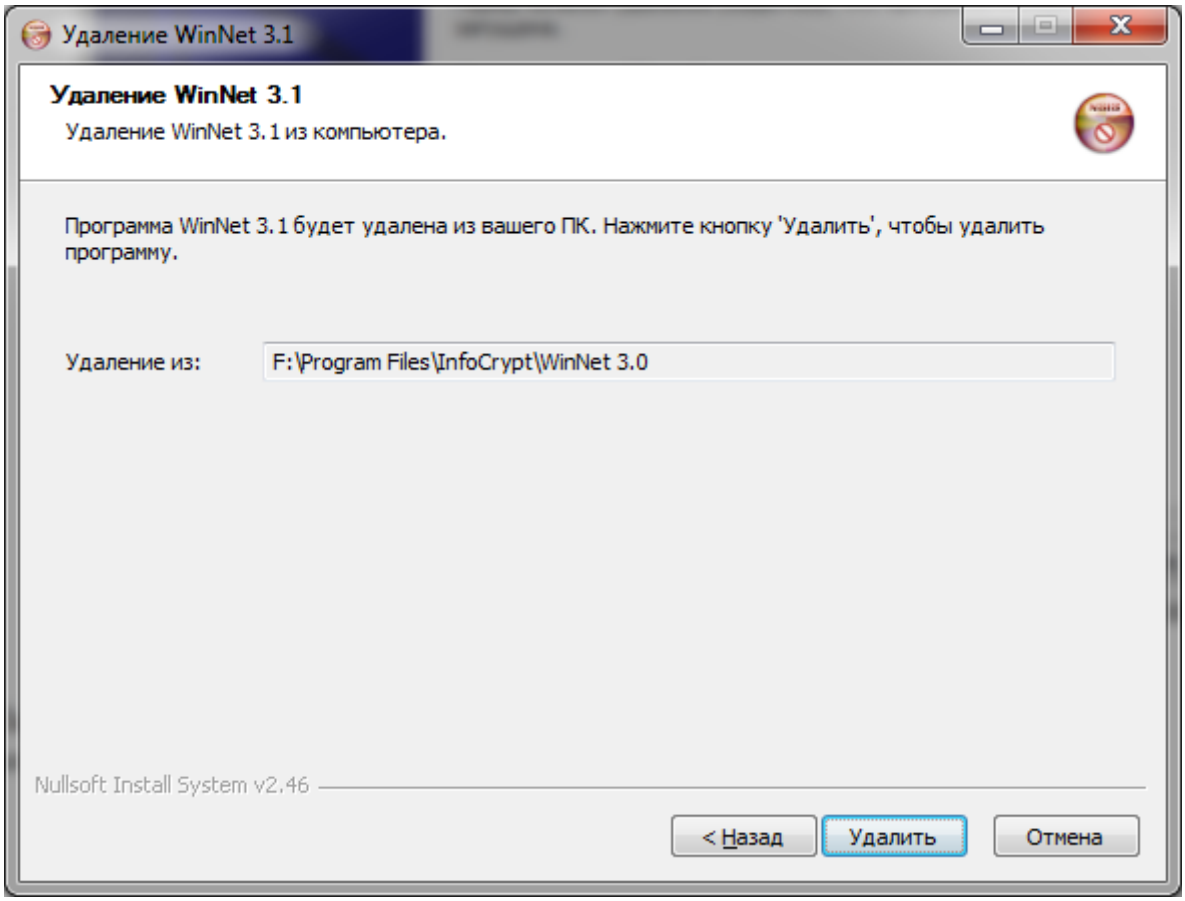


Рисунок 22. Предупреждение о предстоящем удалении ПО "WinNET 3.1"

Затем на экране появится еще одно окно, требующее подтверждения - Рисунок 22 – пользователю требуется кликнуть на одну из кнопок "Удалить" или "Отмена".



И, наконец, появится окно, свидетельствующее о завершении процесса удаления ПО "WinNET 3.1" - Рисунок 23.

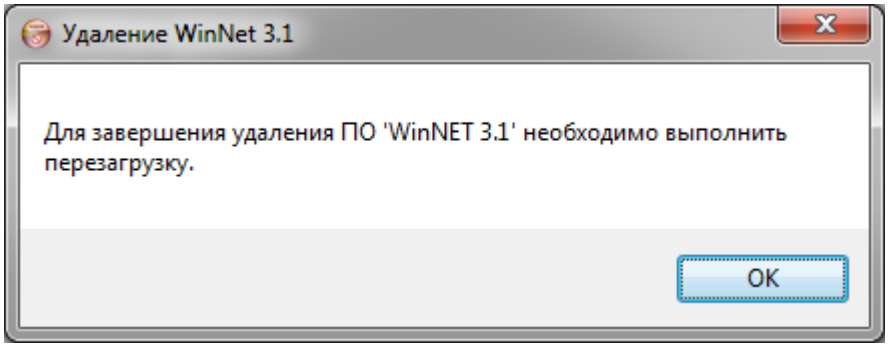


Рисунок 23.

Подключение к домену Windows через службу удаленных терминалов

Необходимо, чтобы на сервере была установлена конфигурация " WinNET 3.1 Сервер", а на клиенте " WinNET 3.1 Клиент".

При подключении к удаленному серверу через клиента MS Terminal Services Client, у пользователя открывается диалоговое окно ввода аутентификационных данных (Рисунок 24):

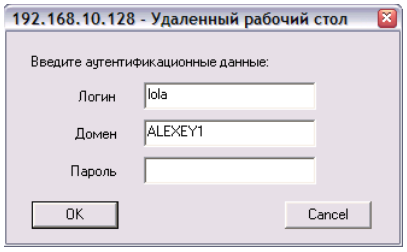


Рисунок 24. Окно ввода аутентификационных данных.

После введения данных и нажатия на кнопку "OK" будет показан запрос на считывание TM/VPN-Key ключа, а затем данные будут переданы на сервер. После отправки данных, в окне MS TSC клиента появится обычный экран удаленного рабочего окна с уже введенными в окно входа в систему доменом, логином и паролем.

По "WinNET 3.1" запоминает последнюю введенную пару Домен/Логин для каждого IP адреса и при следующем обращении к серверу TS по этому адресу подставляет Домен/Логин в окно автоматически.

История изменений

3.1.0.7 Добавлена опция "Установить фильтры WinNet"

3.1.0.8 На tiles от WinNet рисуется версия не 3.0, а 3.1.

3.1.0.9 Добавлена опция /AT - "Пароль любого типа".

3.1.1.5 Начиная с этой версии "WinNET 3.1" работает на Windows 10.

Изменена логика при смене пароля: показываются только те типы пароля, которые были выбраны при установке WinNET. Это ограничение касается только обычных пользователей, администраторы могут устанавливать пароли любого типа.

Приложение 1.

Библиотека WinNetDevice.dll

Функция ReadDomainPassword

Эта функция имеет следующий интерфейс:

```
INT ReadDomainPassword ( CHAR *cDomainName, CHAR *cKbdPassword,
                         CHAR *cPassword )
```

Функция ReadDomainPassword считывает пароль для **текущего пользователя** и заданных имени домена и клавиатурной составляющей пароля. В процессе считывания на экране появляется приглашение приложить устройство – Рисунок 8. В случае успешного считывания как обычно появляется подтверждение – Рисунок 9.

Здесь:

[in] CHAR *cDomainName – задаваемое пользователем имя домена. Если cDomainName == NULL или заданная строка cDomainName пустая (*cDomainName == “”), то используется имя домена (или компьютера) текущего пользователя, которым запущен текущий процесс.

Имя домена может иметь вид UserName\DomainName (или UserName@DomainName). В таком случае в качестве имени домена будет использоваться DomainName, а в качестве имени пользователя – **имя текущего пользователя**.

[in] CHAR *cKbdPassword – клавиатурная компонента пароля. Возможны следующие варианты использования этого параметра:

- cKbdPassword != NULL и * cKbdPassword != "" (cKbdPassword не пустая строка). В таком случае в качестве способа формирования пароля используется “Совместный пароль” и строка cKbdPassword используется как клавиатурная компонента пароля.
- cKbdPassword == NULL. В таком случае в качестве способа формирования пароля используется “Совместный пароль”, а клавиатурная компонента пароля вводится пользователем в появляющемся в таком случае диалоге – Рисунок 25.
- *cKbdPassword == "". В таком случае в качестве способа формирования пароля используется “TM”.

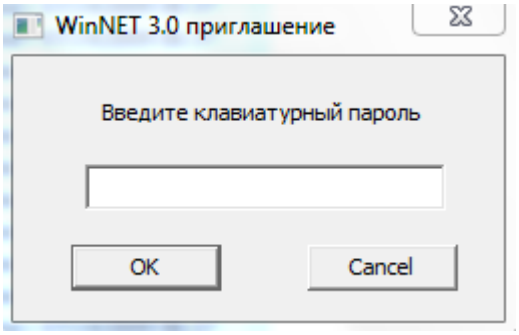


Рисунок 25. Приглашение ввести клавиатурную компоненту пароля в случае cKbdPassword == NULL

[out] CHAR *cPassword – результат работы функции, то есть пароль, сформированный в соответствии с заданным значением параметра cKbdPassword.

Возвращаемое значение: 1 – если требуемый пароль успешно считан, 0 – в противном случае.

При установке ПО “WinNET 3.1” в директорию C:\Program Files\InfoCrypt помещается файл WinNetDevice.lib, который необходимо прилинковать к проекту для implicit вызова функции ReadDomainPassword

Функция ReadDomainPassword2

Эта функция имеет следующий интерфейс:

```
INT ReadDomainPassword2 ( CHAR *cDomainName, CHAR *cUserName,
                          CHAR *cKbdPassword, CHAR *cPassword )
```

Эта функция отличается от ReadDomainPassword тем, что у нее есть еще один аргумент - CHAR *cUserName, в котором задается имя пользователя. В остальном ее функциональность совпадает с функцией ReadDomainPassword: она считывает пароль для **заданного пользователя** и заданных имени домена и клавиатурной составляющей пароля. В процессе считывания на экране появляется приглашение приложить устройство – Рисунок 8. В случае успешного считывания как обычно появляется подтверждение – Рисунок 9.

Здесь:

[in] CHAR *cDomainName – задаваемое пользователем имя домена. Если cDomainName == NULL или заданная строка cDomainName пустая (*cDomainName == ""), то используется имя домена (или компьютера) текущего пользователя, которым запущен текущий процесс.

Имя домена может иметь вид UserName\DomainName (или UserName@DomainName). В таком случае в качестве имени домена будет использоваться DomainName, а в качестве имени пользователя – UserName.

[in] CHAR *cUserName – задаваемое имя пользователя, под которым текущий пользователь хочет аутентифицироваться в приложении. Это имя не обязано совпадать с именем текущего пользователя.

[in] CHAR *cKbdPassword – клавиатурная компонента пароля. Возможны следующие варианты использования этого параметра:

- cKbdPassword != NULL и *cKbdPassword != "" (cKbdPassword не пустая строка). В таком случае в качестве способа формирования пароля используется "Совместный пароль" и строка *cKbdPassword используется как клавиатурная компонента пароля.

- cKbdPassword == NULL. В таком случае в качестве способа формирования пароля используется "Совместный пароль", а клавиатурная компонента пароля вводится пользователем в появляющемся в таком случае диалоге – Рисунок 24.

- *cKbdPassword == "". В таком случае в качестве способа формирования пароля используется “TM”.

[out] CHAR *cPassword – результат работы функции, то есть пароль, сформированный в соответствии с заданным значением параметра cKbdPassword.

Возвращаемое значение: 1 – если требуемый пароль успешно считан, 0 – в противном случае.

Библиотека accnetsb.dll

Библиотека accnetsb.dll предназначена для обеспечения преемственности с ПО "Аккорд WinNET 2.0". Она экспортирует две функции ReadDomainPassword и ReadDomainPassword2, имеющие такой же интерфейс вызова и соглашения о возвращаемых значениях, как соответствующие функции "Аккорд WinNET 2.0".

Функция ReadDomainPassword

Функция, реализующая функционал одноименной функции пакета "Аккорд WinNET 1.0". Обеспечивает совместимость с "Аккорд WinNET 2.0" программ, разработанных для ПО "Аккорд WinNET 1.0". Функция предназначена для чтения пароля пользователя с ключевого носителя комплекса WinNET.
Аргументы функции:

```
int   ReadDomainPassword( char *Domain, char *KbdPassword, char *Password )
```

[in] Domain – имя домена. В случае если Domain – пустая строка, либо NULL – используется домен текущего пользователя, которым запущен процесс, использующий библиотеку accnetsb.dll.

Имя домена может иметь вид UserName\DomainName (или UserName@DomainName). В таком случае в качестве имени домена будет использоваться DomainName, а в качестве имени пользователя – **имя текущего пользователя**.

[in] KbdPassword – Клавиатурный пароль. Параметр может принимать значение NULL, тогда библиотека accnetsb.dll сама выведет окно с запросом клавиатурного пароля.

[out] Password – буфер для сохранения считанного пароля. Буфер должен иметь размер не менее 32 байт.

В случае успешного считывания пароля, функция возвращает 1, в случае ошибки – 0.

Функция ReadDomainPassword2

Функция предназначена для чтения пароля пользователя с ключевого носителя комплекса "WinNET 3.1".

Аргументы функции:

```
int ReadDomainPassword2
```

(char *Domain, char *UserName, char *KbdPassword, char *Password)

[in] Domain –имя домена. В случае если Domain – пустая строка, либо NULL – используется домен текущего пользователя, которым запущен процесс, использующий библиотеку accnetsb.dll.

Имя домена может иметь вид UserName\DomainName (или UserName@DomainName). В таком случае в качестве имени домена будет использоваться DomainName, а в качестве имени пользователя - UserName.

[in] UserName – имя пользователя, для которого считывается пароль.

При предъявлении TM с паролем, созданным на версии 1.x, из TM читается пароль для домена Domain (либо для текущего, в котором запущен процесс, использующий библиотеку acnetsb.dll, если Domain = NULL или Domain = “” – пустая строка) не зависимо от значения, переданного в параметр *UserName.

[in] KbdPassword – Клавиатурный пароль. Параметр может принимать значение NULL, тогда библиотека accnetsb.dll сама выведет окно с запросом клавиатурного пароля.

[out] Password – буфер для сохранения считанного пароля. Буфер должен иметь размер не менее 32 байт.

В случае успешного считывания пароля, функция возвращает 0, в случае ошибки – код ошибки.

Коды ошибок:

```
WNET_INVALID_DU      1 // недопустимое имя домена/пользователя
WNET_DRIVER          3 // не загружен драйвер Accord
WNET_CANCEL          4 // пользователь отказался от ввода
WNET_INVALIDTM       5 // TM не предназначена для работы с WinNET
WNET_NOTFOUND        6 // пароль на носителе не найден
```

Примеры вызова функции ReadDomainPassword2:

ReadDomainPassword2("Domain001", "User001", KbdPassword, Password) – будет возвращен пароль соответствующей указанной паре "Domain001\User001"

ReadDomainPassword2("", "User001", KbdPassword, Password) – будет возвращен пароль пользователя "User001" для домена, в котором запущен процесс, использующий библиотеку accnetsb.dll.

Приложение 2.

Максимальное количество паролей

В следующей ниже таблице приводятся значения максимального количества паролей (в формате "Аккорд WinNET 2.0"), в зависимости от типа устройства TM.

Тип устройства	Максимальное количество паролей
DS1992	Ни одного
DS1993	5
DS1994	5
DS1995	70
DS1996	325

Фирма "ООО ИнфоКрипт"