ОСОБОЕ КОНСТРУКТОРСКОЕ БЮРО
СИСТЕМ АВТОМАТИЗИРОВАННОГО ПРОЕКТИРОВАНИЯ

УТВЕРЖДЕН
37222406.26.20.40.140.091 98-ЛУ

Специальное программное обеспечение средств защиты информации от несанкционированного доступа «АККОРД-Win64 К»

РУКОВОДСТВО ПО УСТАНОВКЕ

37222406.26.20.40.140.091 98

АННОТАЦИЯ

Установка специального программного обеспечения средств защиты информации от несанкционированного доступа (СПО СЗИ НСД) «Аккорд-Win64 K» (ТУ 26.20.40.140-091-37222406-2020) (далее по тексту – СПО «Аккорд-Win64 K», «Аккорд-Win64 K», СПО «Аккорд», «Аккорд») и его настройка с учетом особенностей политики информационной безопасности, принятой на объекте информатизации, осуществляется, как правило, специалистами по защите информации организации (предприятия, фирмы и т.д.) в соответствии с требованиями эксплуатационной документации на СПО «Аккорд-Win64 K».

В документе приведен порядок установки СПО «Аккорд».

Перед установкой и эксплуатацией СПО «Аккорд» необходимо внимательно ознакомиться с комплектом эксплуатационной документации на СПО «Аккорд», а также принять необходимые защитные организационные меры, рекомендуемые в документации.

Применение защитных мер СПО «Аккорд» должно дополняться общими мерами технической безопасности.

ВНИМАНИЕ! Перед началом установки СПО «Аккорд-Win64 K» рекомендуется подробно ознакомиться с эксплуатационной документацией, прежде всего с «Описанием применения» (37222406.26.20.40.140.091 31) и настоящим Руководством.

СОДЕРЖАНИЕ

1. Условия применения СПО «Аккорд»

1.1. Технические требования

Для установки СПО «Аккорд-Win64 K» требуется следующий минимальный состав технических и программных средств:

- установленная 64-битная ОС Windows 7, Windows 8, Windows 8.1, Windows Server 2012 Enterprise Edition R2, Windows 10 Professional, Windows Server 2016 Enterprise Edition, Windows Server 2019 или 32-битная ОС Windows 7, Windows 8, Windows 8.1, Windows 10 Professional;
- объем свободного дискового пространства для установки СПО «Аккорд» – не менее 20 Мб;
- наличие CD ROM для установки СПО разграничения доступа;

При применении СПО «Аккорд» на рабочей станции количество пользователей, регистрируемых на одном СВТ, не должно превышать 3000 человек. При использовании СПО «Аккорд» для защиты систем терминального доступа возможна регистрация до 1024 пользователей.

1.2. Организационные меры

Для эффективного применения средств защиты комплекса и поддержания необходимого уровня защищенности СВТ и информационных ресурсов АС необходимы:

- физическая охрана СВТ и его ресурсов;
- наличие администратора безопасности информации (администратор БИ) - привилегированного пользователя, имеющего особый статус и абсолютные полномочия (супервизора). Администратор БИ должен организовать установку СПО в СВТ, настройку защитных механизмов в соответствии с правами доступа пользователей, осуществлять контроль за правильным использованием СВТ с установленным СЗИ;
- использование в СВТ технических и программных средств, сертифицированных как в Системе ГОСТ Р, так и в ГСЗИ;
- запрет на использование в СВТ любых сторонних служб и протоколов, позволяющих осуществить удаленный доступ к подконтрольным объектам (Telnet, SSH, TeamView, RemoteDesktop и т.д.).

2. Порядок установки СПО «Аккорд»

Установка СПО «Аккорд» (ТУ 26.20.40.140-091-37222406-2020) включает следующие этапы:

1. Установка на жесткий диск специального программного обеспечения разграничения доступа с дистрибутивного носителя.
2. Копирование ключевого файла лицензии.
3. Назначение правил разграничения доступа (ПРД) для пользователей в соответствии с политикой информационной безопасности, принятой в организации, и активация подсистемы разграничения доступа с помощью программы настройки СПО «Аккорд» (ACSETUP.EXE).

Примечание: В ОС Windows 10 СПО «Аккорд» может работать некорректно. Для предотвращения возможных осложнений в работе перед установкой СПО рекомендуется отключить в СВТ функцию быстрого запуска ОС, используя следующий алгоритм действий:

1) разблокировать встроенную в ОС учетную запись "Администратор";
2) при перезапуске войти в ОС под этой учетной записью;
3) в настройках электропитания отключить переход в спящий режим;
4) выполнить команду *powercfg.exe /h off*;
5) значение параметра реестра
HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\Power\HiberbootEnabled
сделать равным 0.

2.1. Установка СПО разграничения доступа «Аккорд» на жесткий диск

2.1.1. Общие сведения

Установка СПО на жесткий диск СВТ осуществляется в следующей последовательности:

1. Загрузить ОС с правами Администратора;
2. С компакт-диска «Аккорд» запустить программу AccordSetupWin64-K.exe (AccordSetup-K.exe – для 32-битных ОС). Процесс установки локальной и терминальной версий выглядит одинаково, различается только содержимое ключевого файла лицензии.
3. Выбрать логический диск и каталог для установки СПО «Аккорд». По умолчанию установка выполняется в папку C:\ ACCORD.X64 (C:\ACCORD.NT – для 32-битных ОС), но администратор может выбрать другие варианты по своему усмотрению. Программа создаст на заданном логическом диске папку C:\ACCORD.X64 (C:\ACCORD.NT – для 32-битных ОС) (или имя, заданное администратором) со всеми необходимыми подкаталогами и скопирует туда программное обеспечение.

На данном этапе в составе ОС не производится никаких изменений, кроме создания каталогов или файлов на жестком диске.

Примечание: При использовании версии СПО «Аккорд» 5.0.10.71 (64-битные ОС) или 4.0.10.71 (32-битные ОС) может потребоваться дополнительное действие для СВТ с определенной версией ОС. Если информация о версии ОС, выводимая командой VER, отображается в формате 10.0.XXX.XXXX, то после установки СПО перед началом работ по настройке комплекса необходимо произвести перезапись файла Accord.dat из каталога установки ACCORD.X64 (ACCORD.NT для 32-битных ОС), заменив его на аналогичный файл из каталога ACCORD.DAT\X64\ (ACCORD.DAT\X32\) с диска поставки.

4. Запустить программу «Настройка идентификаторов Аккорд» и выполнить необходимые настройки (подробнее см. 2.1.2).

5. Получить файл лицензии (см. 2.1.3), скопировать его в папку с установленными файлами СПО «Аккорд-Win64 K» под именем «accord.key». Рекомендуется сохранить резервную копию файла accord.key.

6. Запустить программу «Настройка комплекса Аккорд» (AcSetup.exe из папки с установленным ПО СЗИ «Аккорд») и выполнить необходимые настройки. Завершить работу программы с сохранением изменений. Необходимо помнить, что выбранные настройки вступят в силу только после перезагрузки СВТ, на котором установлено СПО «Аккорд». Активации подсистемы разграничения доступа СПО «Аккорд» на данном этапе не требуется.

В случае если Администратор БИ не является Администратором ОС Windows, он может запустить программу «Настройка комплекса Аккорд», но при ее запуске на экране появится сообщение (рисунок 1):

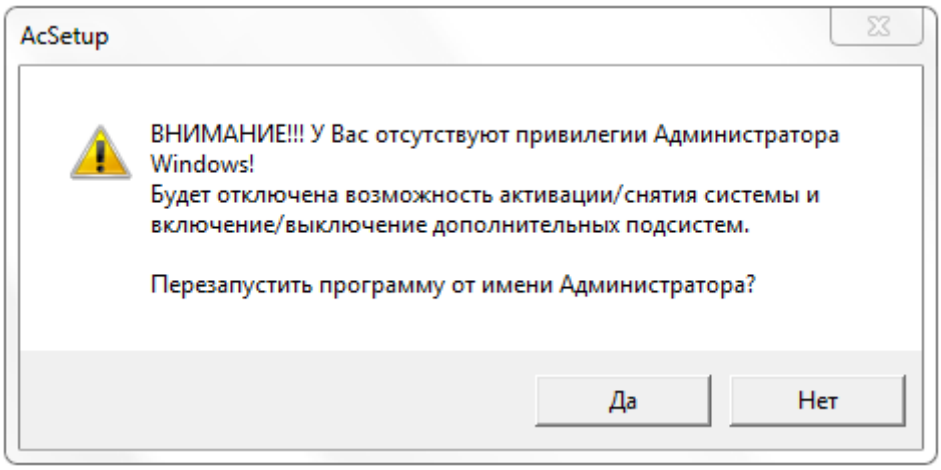


Рисунок 1 – Сообщение, возникающее при запуске программы не Администратором ОС Windows

Если в этом сообщении выбрать кнопку <Да> (т.е. перезапуск программы от имени Администратора ОС Windows), то появляется окно, в котором будет предложено ввести имя и пароль Администратора ОС Windows (рисунок 2).

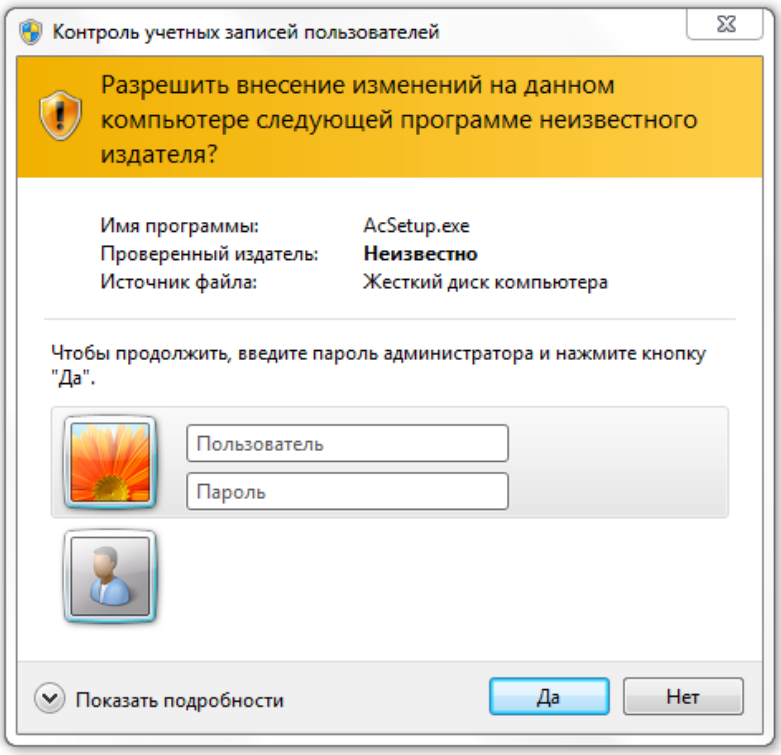


Рисунок 2 – Окно ввода пароля Администратора ОС Windows

При успешной авторизации появляется главное окно программы настройки СПО «Аккорд», в которой будут доступны все функции (п. 2.2.2).

Если в сообщении на рисунке 1 выбрать кнопку <Нет> (т.е. продолжить запуск программы AcSetup.EXE), то на экране появляется главное окно программы настройки СПО «Аккорд», в которой некоторые функции будут заблокированы. Список заблокированных функций:

а) в главном окне программы настройки СПО «Аккорд»:

- Перезагрузка при ошибках;
- Спрашивать разрешение;
- Проверять BOOT сектора;
- Поддержка USB клавиатуры;

б) во вкладке «Команды»:

- Активация;
- Снятие;

в) во вкладке «Параметры»:

- Язык;

г) во вкладке Параметры\Дополнительные\Контроль:

- Включить подсистему контроля имен общих ресурсов;
- Включить подсистему контроля доступа к общим ресурсам;

д) во вкладке Параметры\Дополнительные\Режим сессии:

- Режим старта системы защиты;
- Запретить загрузку ОС в безопасном режиме;
- Переключение монитора в текстовый режим при старте;

– Вести журналы в;

– Изменить экран входа в систему;

е) во вкладке Параметры\Дополнительные\Разное:

– Текст в хранителе экрана.

7. Запустить программу редактора ПРД. Начиная с версии V5.0.10.93 (для 64-битных ОС) в СПО «Аккорд» включены два редактора ПРД – Aced32 (C:\ACCORD.X64\Aced32.exe) и AcedVI (C:\ACCORD.X64\AcedVI.exe). В появившемся на экране сообщении (при запуске Aced32: «Файл \Accord.64\Accord.amz не найден. Создать новый?» или «Файл \Accord.NT\Accord.amz не найден. Создать новый?» – для 32-битных ОС; при запуске AcedVI: «Файл БД не найден. Создать новый?») выбрать кнопку <Да>. Далее назначить ПРД в соответствии с принятой политикой информационной безопасности и полномочиями пользователей. Описание редакторов ПРД приведено в документах «Установка правил разграничения доступа. Программа ACED32. Руководство пользователя» (37222406.26.20.40.140.091 97) и «Редактор прав пользователей виртуальной инфраструктуры. Программа AcedVI» (11443195.4012-037 97) в составе эксплуатационной документации на СПО «Аккорд-Win64 К».

8. Провести активацию подсистемы разграничения доступа СПО «Аккорд». Для этого в программе «Настройка комплекса Аккорд» необходимо выполнить команду меню Команды\Активация.

В СПО «Аккорд-Win64 К» имеется поддержка стороннего модуля, необходимого для получения пользовательских учетных записей для входа в систему (CredentialProvider компании «Аладдин Р.Д.»). При наличии такого модуля во время выполнения процедуры активации СПО «Аккорд» посредством программы AcSetup.EXE на экране появляется сообщение: «Выберите дополнительные CredentialProvider для входа:

– AcGina;

- SLCredentialProvider.»

Для работы с СПО «Аккорд-Win64 К» необходимо выбрать хотя бы один модуль.

Если выбран пункт «AcGina», то процедуры И/А выполняются за счет модуля AcGina.

Если выбран пункт «SLCredentialProvider», то процедуры И/А выполняются за счет модуля компании «Аладдин Р.Д.».

Если выбраны оба модуля, то пользователю при входе в ОС предлагается выбрать один из вариантов входа в систему: вход посредством СПО «Аккорд-Win64 К» или вход посредством CredentialProvider компании «Аладдин Р.Д.».

Если активация подсистемы разграничения доступа прошла успешно, то на экране появляется окно для настройки подсистемы разграничения доступа СПО «Аккорд» (рисунок 3).

При активированной системе «Аккорд» не рекомендуется выполнять операцию смены языка для программ, не использующих Юникод, а также изменять имя встроенного администратора ОС.

Примечание: В некоторых случаях не требуется выполнения процедуры синхронизации файла ПРД СПО «Аккорд» со списком пользователей ОС. Тогда после выполнения настройки идентификаторов (п.2.1.2) рекомендуется:

– запустить программу «Настройка комплекса Аккорд» (а не редактор прав доступа);

– предъявить идентификатор, в котором записан ключевой файл лицензии;

– снять флаг «Синхронизация с базой пользователей NT» и сохранить изменения;

– выполнить дальнейшие настройки СПО «Аккорд».

Подсистема разграничения доступа «Аккорд» после предъявления идентификатора пользователя «Гл.Администратор» при входе в ОС выполняет поиск администратора в следующем порядке:

- поиск имени «Администратор» (имя найдено–выполняется вход в ОС);
- поиск имени «Administrator» (имя найдено–выполняется вход в ОС);

Если оба имени не найдены, то создается учетная запись «SUPERVISOR», отсутствующая в ОС, при этом вход в ОС выполнить нельзя.

В случае необходимости изменения имени встроенного Администратора ОС следует:

- в программе настройки СПО Аккорд (AcSetup.exe) установить флаг «Использовать полное имя в учетных записях NT»;
- на компьютере в Панели управления\Учетные записи пользователей выбрать учетную запись администратора ОС и ввести измененное имя администратора ОС в поле «Полное имя».

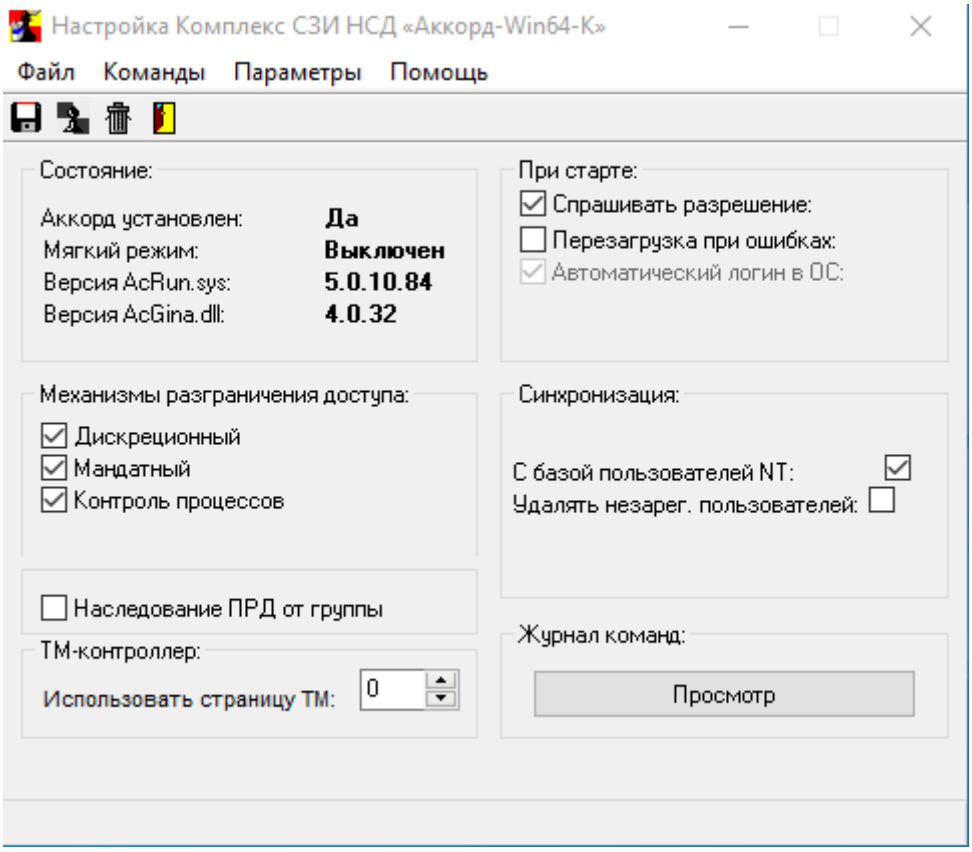


Рисунок 3 – Главное окно программы настройки ПРД

ВНИМАНИЕ! Для корректной работы СПО «Аккорд-Win64 K» и антивирусного ПО необходимо добавить в доверенную зону антивирусного ПО каталог Accord.x64 и следующие системные файлы:

\WINDOWS\SYSTEM32\ACCORD.SCR
\WINDOWS\SYSTEM32\ACGINA.DLL
\WINDOWS\SYSTEM32\ACNP.DLL
\WINDOWS\SYSTEM32\ACRUNNT.EXE
\WINDOWS\SYSTEM32\ACRUNVDD.DLL
\WINDOWS\SYSTEM32\ACRUNYDD.EXE
\WINDOWS\SYSTEM32\ACUSRMOD.DLL
\WINDOWS\SYSTEM32\AZIAHLP.DLL
\WINDOWS\SYSTEM32\DRIVERS\ACBOOT.SYS
\WINDOWS\SYSTEM32\DRIVERS\ACLOCK2K.SYS
\WINDOWS\SYSTEM32\DRIVERS\ACRUN.SYS
\WINDOWS\SYSTEM32\DRIVERS\ACXALLOW.SYS
\WINDOWS\SYSTEM32\DRIVERS\ACXLMSRV.SYS
\WINDOWS\SYSTEM32\TMATTACH.DLL
\WINDOWS\SYSTEM32\TMDRV32.DLL
\WINDOWS\SYSTEM32\ACNP.DLL
\WINDOWS\SYSTEM32\ACUSRM64.DLL

\WINDOWS\SYSTEM32\AZIAH64.DLL \WINDOWS\SYSTEM32\TMATT64.DLL \WINDOWS\SYSTEM32\TMDRV64.DLL

2.1.2. Особенности работы программы «Настройка идентификаторов СЗИ Аккорд»

Совместно с СПО «Аккорд» могут использоваться различные типы идентификаторов: устройства Touch Memory типа DS 1992, 1993, 1996, ПАК «ПИ ШИПКА», Рутокен Lite, Рутокен ЭЦП 2.0, Рутокен 2151, JaCarta, ESMART® Token, USB-Flash-накопитель, Специальный носитель ПО ПАК «Центр-Т». Кроме того, имеется возможность выполнять идентификацию по вводимому логину (идентификатор «Клавиатура»).

Для подключения идентификаторов используется или стандартный USB-порт на материнской плате, или кабель подключается непосредственно к плате контроллера АМДЗ (при его наличии в системе). При этом возможны варианты, когда в составе одной автоматизированной системы (АС) используется несколько видов идентификаторов. Для удобного конфигурирования различных вариантов использования идентификаторов разработана и включена в состав СПО «Аккорд» программа «Настройка идентификаторов СЗИ Аккорд».

Запустить программу настройки можно в процессе инсталляции СПО «Аккорд» на жесткий диск компьютера. После копирования файлов в указанную папку на диске, на экране появляется окно «Завершение работы мастера установки». В этом окне можно включить флаг «Настройка идентификаторов». В состав СПО «Аккорд» по умолчанию включены библиотеки для работы с данным типом идентификаторов. В файле конфигурационных параметров СПО «Аккорд» «accord.ini» используется параметр:

– «DefaultStartType=1» - означает, что монитор безопасности запускается при старте ОС как системный драйвер.

Воспользоваться программой настройки идентификаторов можно и после установки СЗИ от НСД «Аккорд». Для этого достаточно пройти процедуру идентификации/аутентификации и начать сеанс работы под учетной записью, которая входит в группу «Администраторы» в составе СЗИ «Аккорд», и в составе ОС.

Учетная запись «Гл.Администратор» (SUPERVISOR) СЗИ «Аккорд» по умолчанию синхронизируется со встроенной учетной записью «Администратор» (Administrator) в составе операционной системы.

Запустить программу «Настройка идентификаторов Аккорд» (AcIdCfg.exe) можно из подкаталога «Identifiers», который копируется в основной каталог СПО Аккорд в процессе установки.

Также программу можно запустить через меню Пуск –> Программы –> Аккорд –> Настройка идентификаторов Аккорд.

После запуска открывается основное окно программы (рисунок 4)

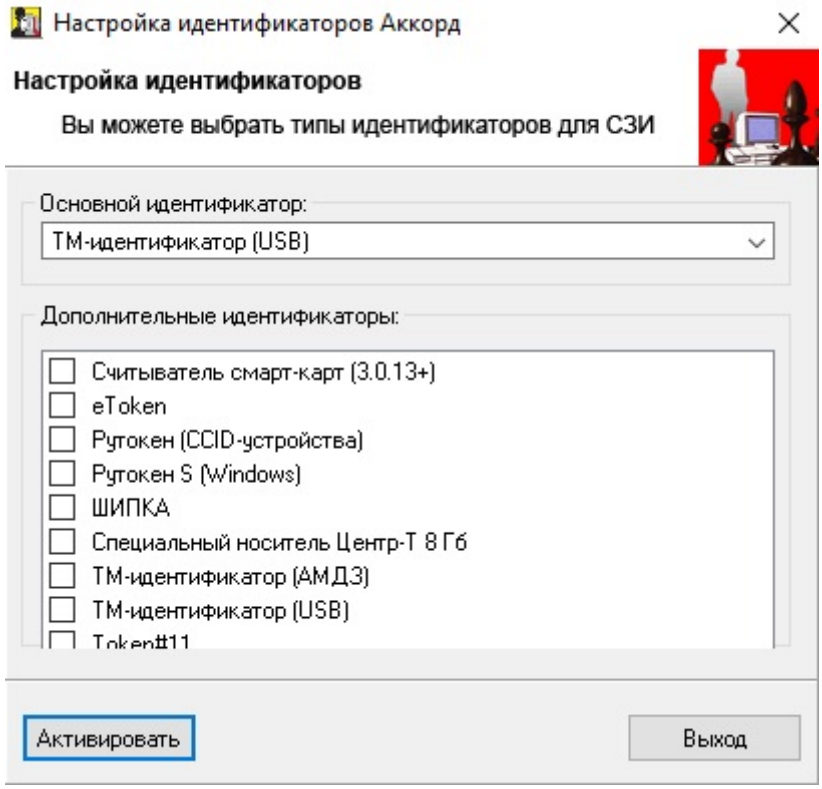


Рисунок 4 – Главное окно программы «Настройка идентификаторов Аккорд»

В главном окне программы необходимо установить основной идентификатор.

Если необходимо использовать **несколько идентификаторов одновременно**, в поле «Дополнительные идентификаторы» нужно выбрать один или несколько дополнительных идентификаторов и нажать кнопку <Установить>. После этого программа копирует в системную папку Windows/System32/ те библиотеки, которые предназначены для поддержки выбранных типов идентификаторов. Если процедура установки прошла успешно, на экран выводится следующее оповещение (рисунок 5).

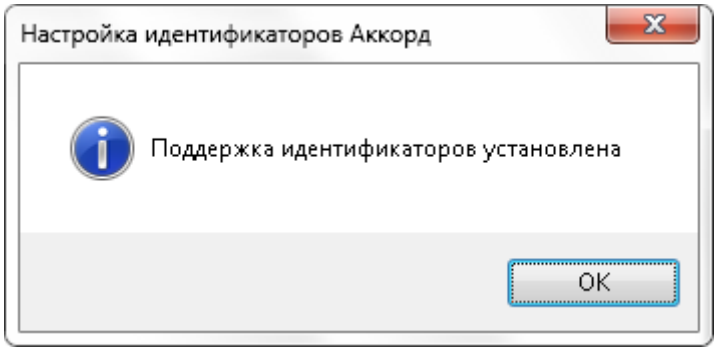


Рисунок 5 – Оповещение об успешном выполнении процедуры поддержки идентификаторов

Администратор может выбрать **любые типы идентификаторов в качестве основных**. Для этого нужно нажать на стрелку в правой части поля «Основной идентификатор» и в выпадающем списке выбрать нужное значение.

Если в качестве основного выбирается «ТМ-идентификатор (АМДЗ)»[1], программа настройки комплекса «Аккорд» будет сравнивать значение ключа в файле лицензии с теми значениями, которые считываются из платы АМДЗ. На платах Аккорд-5мх rev.8 и Аккорд-5.5 rev.8 устанавливается микросхема, которая содержит уникальный, неизменяемый код (UID). В файле лицензии для таких контроллеров прописывается именно это значение в поле «SerialNumber=». В составе контроллеров 5, 5MX, 5.5 более ранних релизов и в составе контроллеров LE, GX, GXM, GXMH, GXM2 таких микросхем нет, и файл лицензии оформляется на серийный номер платы.

Если в рамках работы с виртуальной машиной подключение к виртуальному терминальному серверу планируется только удаленно, рекомендуется в программе «Настройка идентификаторов Аккорд» не устанавливать дополнительные идентификаторы, выбрав в качестве основного идентификатора «Виртуальная машина». Описанная рекомендация применима только в том случае, когда на виртуальном терминальном сервере установлена серверная часть СПО «Аккорд» и не установлена клиентская часть ПО.

Если на виртуальном терминальном сервере установлена как серверная часть СПО «Аккорд», так и клиентская часть, необходимо запустить программу AcIdCfg.EXE и выбрать те идентификаторы, которые используются в организации в соответствии с принятым регламентом работы.

После установки типа основного идентификатора программа настройки СПО «Аккорд» сравнивает число в поле «SerialNumber» с некоторым «синтетическим» параметром, который вычисляется от состава операционной системы. Этот параметр (SID компьютера) заранее не известен сотрудникам ОКБ САПР. Поэтому администратор безопасности, который устанавливает СПО «Аккорд» в таком варианте, должен выбрать тип идентификатора, нажать кнопку <Активировать>, подтвердить в следующем окне свой выбор. Далее нужно запустить программу TmExplor.exe.

Данная программа позволяет определить:

- серийный номер идентификатора;
- версию ТМ-драйвера.

Для получения информации о ключе идентификатора необходимо выбрать опцию Команды \ Информация о ТМ. На экране появляется сообщение с информацией о ключе, типе, объеме памяти идентификатора (рисунок 6).

[1] При наличии в системе СЗИ «Аккорд-АМДЗ»

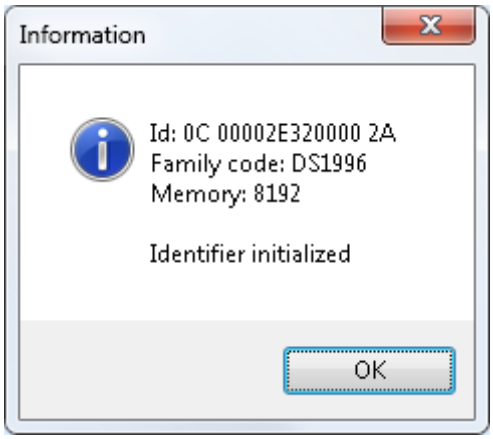


Рисунок 6 – Информация о ключе идентификатора

Если в идентификаторе имеется ключ, то в сообщении появится запись «Identifier initialized» (рисунок 6), если ключ не был записан в идентификатор – «Warning! Identifier not initialized!».

2.1.3. Получение файла лицензии

Получить файл лицензии можно:

1) с помощью программы «Тест для проверки работы контроллера» (TmExplor.exe);

2) с помощью программы LIU.EXE.

С помощью программы «Тест для проверки работы контроллера» (TmExplor.exe): необходимо прислать значение полей «UID» программы «Тест для проверки работы контроллера» по адресу электронной почты key@okbsapr.ru, указав в письме наименование продукта, для которого необходим файл лицензии. Производственный отдел сформирует файл лицензии и отправит его заказчику. Полученный файл нужно скопировать в папку с установленными файлами СЗИ «Аккорд» под именем «accord.key» и продолжить настройку СПО «Аккорд».

С помощью программы «Данные для лицензий» (LIU.EXE):

- запустить программу LIU.EXE;
- в главном окне программы в поле «Аккорд-WinXX» выбрать кнопку <Сгенерировать UID> (или выполнить команду Тип продукта\Аккорд-XX, рисунок 7);

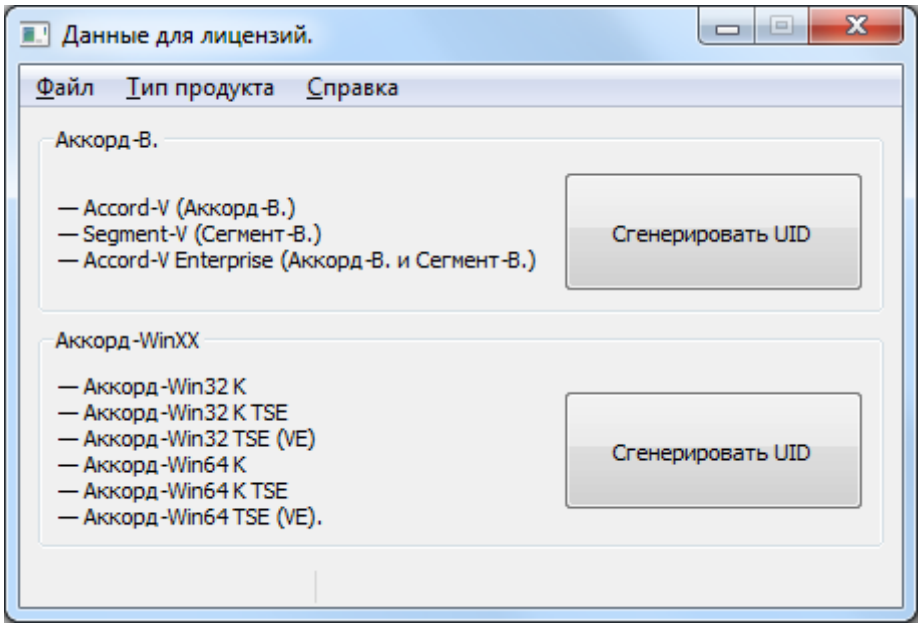


Рисунок 7 – Главное окно программы LIU.EXE

- далее выбрать один из трех вариантов действий:
  - в появившемся на экране окне (рисунок 8) копировать значение поля «UID вашего компьютера» в буфер обмена, а затем прислать его по адресу электронной почты key@okbsapr.ru. Производственный отдел сформирует файл лицензии и отправит его заказчику. Далее полученный файл скопировать в папку с установленными файлами СЗИ «Аккорд» под именем «accord.key»;
  - создать файл с запросом на получение лицензии (файл с данными для лицензии);
  - отправить данные для получения лицензии письмом.

Для создания файла с запросом необходимо в окне, показанном на рисунке 8, указать имя организации, эксплуатирующей СПО «Аккорд», тип продукта СПО «Аккорд», срок действия лицензии, номер договора или счета поставки (последнее поле не является обязательным для заполнения).

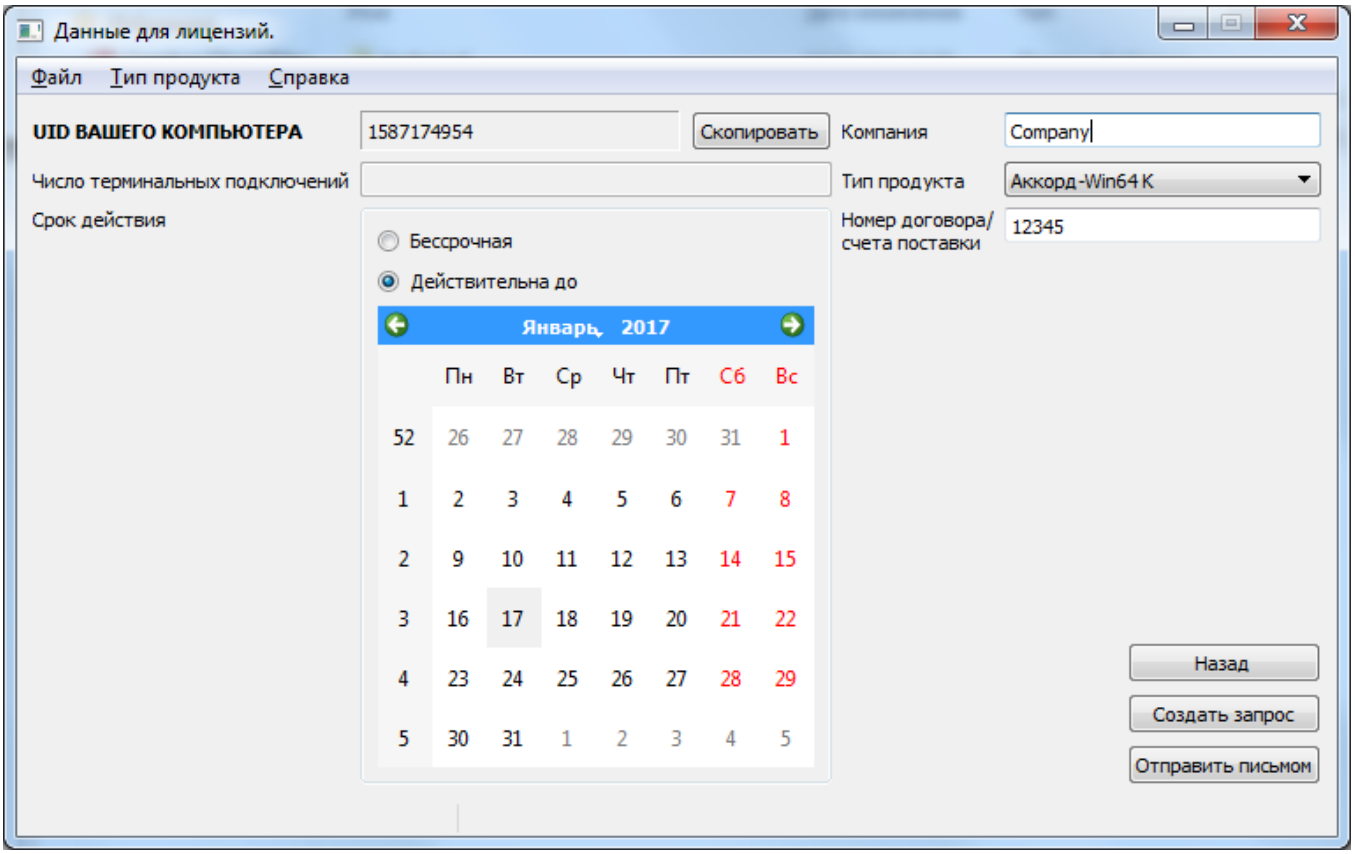


Рисунок 8 – Указание данных для получения файла лицензии

Далее нажать кнопку <Создать запрос>. В случае успешного завершения процедуры на экране появляется окно:

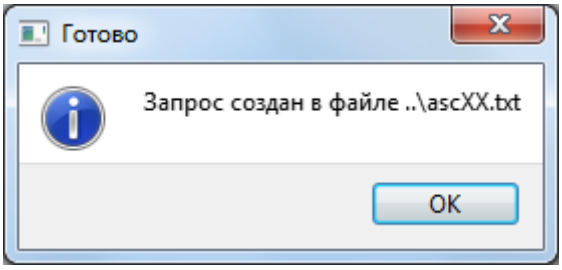


Рисунок 9 – Создание запроса на получение файла лицензии

Файл с запросом на получение лицензии хранится в каталоге с программой «Данные для лицензий».

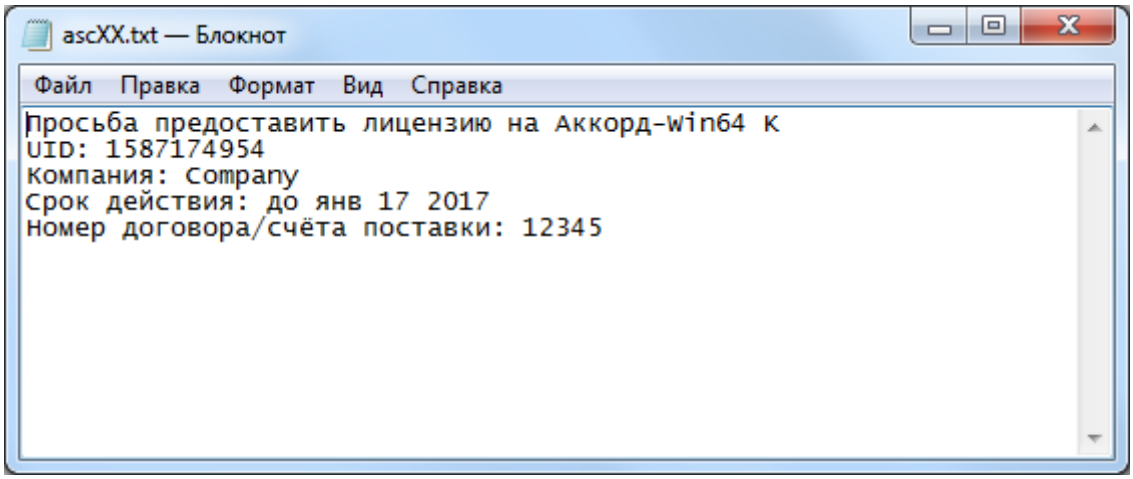


Рисунок 10 – Пример файла с запросом на получение файла лицензии для СПО «Аккорд-Win64 K»

Далее этот файл следует отправить в производственный отдел ЗАО «ОКБ САПР» по адресу электронной почты key@okbsapr.ru.

Чтобы отправить данные для получения лицензии письмом, необходимо нажать кнопку <Отправить письмом> (рисунок 8). После этого на экране появляется окно почтового клиента, установленного на компьютере (при этом автоматически указывается тема письма «UID для лицензии Аккорд-XX», адрес электронной почты, на который необходимо отправить письмо (key@okbsapr.ru), и текст письма – данные о продукте).

2.1.4. Основные параметры настройки СПО «Аккорд»

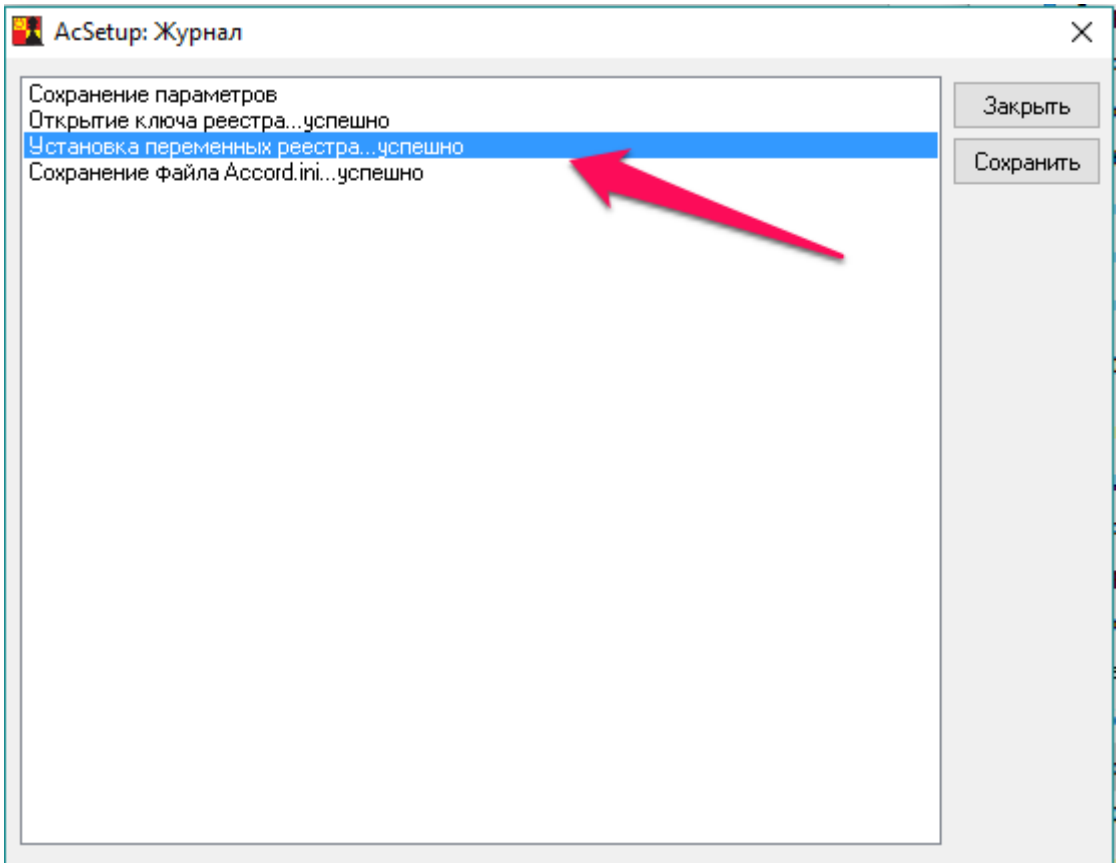
ВНИМАНИЕ! В утилите AcSetup.exe изменение следующих параметров возможно только при активированном комплексе «Аккорд» (поскольку они прописываются в реестре Windows):

– «Спрашивать разрешение»;

– «Перезагрузка при ошибках»;

– «Проверять BOOT сектора».

Успешное изменение этих параметров можно увидеть в журнале команд, нажав кнопку <Просмотр> в поле «Журнал команд» в главном окне утилиты AcSetup.exe:



При неактивированном комплексе «Аккорд» после изменения параметров и повторного запуска утилиты AcSetup.exe параметры будут иметь значения по умолчанию.

В правой части окна программы AcSetup.EXE размещено поле **«При старте»**, предназначенное для задания режимов загрузки «монитора разграничения доступа» – программы ACRUN. SYS. Выбор режима загрузки осуществляется путем установки/снятия соответствующего флага:

«Спрашивать разрешение» – при включении этого режима в момент загрузки ACRUN.SYS выводится запрос и можно отказаться от запуска программы. **Этот режим допустим только на период тестирования системы**.

«Перезагрузка при ошибках» – если установлен этот флаг, то при обнаружении ошибок (например, пользователь не зарегистрирован в базе данных) происходит принудительная перезагрузка. **Это основной режим функционирования системы разграничения доступа!** В том случае, когда установлен такой режим работы системы защиты и возникает ошибка, не позволяющая продолжить загрузку, для администратора предусмотрен резервный механизм отключения старта монитора безопасности. Действует он только для пользователя «Гл. Администратор» и для его корректной работы в настройке СПО «Аккорд» в параметре «Результаты И/А» должны быть включены первые пять флагов.

ВНИМАНИЕ! При включении опции «Перезагрузка при ошибках» (а она обязательно должна быть включена при штатном функционировании СПО «Аккорд») автоматически запрещается загрузка в безопасном режиме.

ВНИМАНИЕ! Принудительная перезагрузка компьютера, выполняемая при обнаружении ошибок (с установленным флагом «Перезагрузка при ошибках»), может быть интерпретирована операционной системой как некорректное завершение работы. Данная особенность взаимодействия ОС и СПО «Аккорд» является штатной.

«Автоматический логин в ОС» - при включении этого режима в момент загрузки модуль ACGINA.DLL получает информацию о пользователе, который был идентифицирован СПО «Аккорд». При этом вход в систему может осуществляться двумя способами:

- подсистема доступа получает имя пользователя. Первые четыре флага установлены в разделе «Результаты I/A» параметров пользователя. В этом случае при логине в ОС требуется ввести с клавиатуры пароль пользователя. Имя пользователя изменить нельзя.
- подсистема доступа получает имя и пароль пользователя (первые пять флагов установлен в разделе «Результаты И/А»). В этом случае при логине в ОС ввода пароля не требуется.

ВНИМАНИЕ! Для вступления в силу изменений параметров в поле «При старте» необходима перезагрузка СВТ.

Если СВТ подключено к сети, то у пользователя есть возможность выбрать имя домена или сервера, к которому он может получить доступ, даже если включен параметр «Автологин». Для этого администратору перед активацией подсистемы разграничения доступа нужно включить расширенный режим входа в систему (кнопка <Параметры> в стандартном окне запроса имени и пароля пользователя).

В случае необходимости одновременного использования флага «Автоматический логин» и параметра ScreenSaver «Блокировать компьютер» рекомендуется установить флаг «Не запрещать автоматический логин в ОС» (см. документ «Установка правил разграничения доступа. Программа ACED32» 37222406.26.20.40.140.091 97).

В терминальной версии СПО «Аккорд-Win64 K» флаг «Автоматический логин в ОС» установлен по умолчанию, отключить его нельзя.

«Наследование ПРД от группы»[2] – если данный флаг установлен, то при загрузке правил разграничения доступа сначала загружаются ПРД, установленные для группы пользователей, а затем на них «накладывается» ПРД пользователя. В таком режиме в программе ACED32 отключается

[2)] Данный функционал доступен в ПО «Аккорд» начиная с версии x.0.10.51

синхронизация между группой и пользователем по полям «Объекты» и «Процессы».

Флагу «Наследование ПРД от группы» соответствует параметр NtAccessStyle в файле Accord.ini.

Поле **«Синхронизация»** определяет режимы синхронизации базы данных пользователей. Флаг ***«С базой пользователей NT»*** определяет режим, при котором программа-редактор добавляет пользователей СЗИ «Аккорд» в базу операционной системы. Этот флаг необходим, если включен режим «Автоматический логин в ОС», и пользователи, зарегистрированные в СЗИ «Аккорд», отсутствуют в списке пользователей ОС. Этот флаг можно не включать, если в «Аккорде» регистрируются пользователи, которые уже включены в состав контроллера домена или зарегистрированы на терминальном сервере.

Примечание: учетная запись «Гл.администратор» автоматически синхронизируется с системной учетной записью «Администратор» в русской версии Windows или с записью «Administrator» в английской версии. Если в составе ОС учетная запись «Администратор» отсутствует, то СЗИ «Аккорд» создает запись Supervisor и включает ее в группу «Администраторы». Если в составе ОС учетная запись «Администратор» существует, но заблокирована, то СЗИ «Аккорд» разблокирует эту запись и синхронизируется с ней.

«Удалять незарегистрированных пользователей» – установка этого дополнительного флага определяет способ синхронизации пользователей СЗИ «Аккорд» с базой ОС Windows. Если флаг не установлен, то пользователи СЗИ просто добавляются в базу пользователей ОС. Если флаг установлен, то в базе пользователей операционной системы останутся ТОЛЬКО пользователи СЗИ «Аккорд».

При установленной СЗИ «Аккорд» в автоматизированной системе (компьютер + ПО) появляются 2 базы пользователей: база в составе СПО «Аккорд» (файл Accord.AMZ) и база учетных записей в составе ОС. Следующий флаг отвечает за синхронизацию этих баз:

- **«синхронизация с NT»**[3]. Если установлен этот флаг, то при выходе из редактора Aced32 созданные пользователи заносятся в базу пользователей ОС. В этот момент проверяется флаг «Удалять незарегистрированных пользователей». Если он установлен, и если в ОС зарегистрированы пользователи, не существующие в Accord.AMZ, то эти пользователи удаляются из базы NT. При этом администратор должен позаботиться о том, чтобы политики парольной защиты (минимальная длина, набор символов, срок действия) совпадали в настройках политики ОС и СЗИ «Аккорд».

Таким образом, если включены 2 флага синхронизации: «с NT» + «Удалять незарегистрированных пользователей», то обе базы становятся идентичными по именам пользователей и паролям. Если флаги не установлены, то возможны случаи, когда в одних базах будет больше/меньше пользователей, чем в других, а пароли одного и того же пользователя будут различны для

[3] При работе с редактором AcedVI флаг не используется, а соответствующий ему параметр в файле Accord.ini – UseNTBase – рекомендуется выставить в значение No

работы с СПО «Аккорд» и для загрузки ОС. В этом случае нужно отключить флаг «Автологин», или убрать передачу пароля в «Результатах И/А».

Если все пользователи работают в домене, и локальный вход не нужен (или вообще запрещен), то синхронизацию с базой NT можно смело убирать. В настройках СПО «Аккорд» нужно включить флаги «Использовать полное имя в учетных записях NT» и «Автологин», а в редакторе ПРД в поле «Полное имя» ввести <доменное имя юзера>@<имя домена>. Единственное ограничение – пароль нужно менять, когда пользователь уже авторизовался на домене через Ctrl-Alt-Del и кнопку <Смена пароля>.

Поле **«Механизмы разграничения доступа»** определяет те методы разграничения доступа, которые будут использоваться при реализации политики безопасности (подробнее о методах разграничения доступа см. документы «Установка правил разграничения доступа. Программа ACED32» и «Редактор прав пользователей виртуальной инфраструктуры. Программа AcedVI»).

В поле **«Идентификатор»** только один параметр – ***«Страница в идентификаторе»***. По умолчанию он установлен в 0. Изменять этот параметр КАТЕГОРИЧЕСКИ НЕ РЕКОМЕНДУЕТСЯ! В эту и следующую страницу памяти идентификатора записывается ключ пользователя при его регистрации. Изменение этого параметра приведет к тому, что ранее зарегистрированные идентификаторы будут восприниматься системой защиты как недопустимые. Изменение этого параметра возможно, если используется ПО сторонних производителей, которое записывает свою информацию в те же страницы памяти. После изменения этого параметра ВСЕ используемые идентификаторы должны быть перерегистрированы с генерацией нового ключа пользователя.

Кнопка <Просмотр> в поле «Журнал команд» активна во время выполнения процедур активации и снятия средств защиты СПО «Аккорд» (при условии, что после выполнения активации или снятии средств защиты СПО «Аккорд» не выполняется перезагрузка СВТ).

При нажатии кнопки <Просмотр> в поле **«Журнал команд»** осуществляется просмотр следующих команд: копирование файлов СПО «Аккорд-Win64 K» при активации СПО «Аккорд», модификация реестра вследствие установки СПО «Аккорд-Win64 K», создание и остановка сервисов Аккорда (рисунок 11).

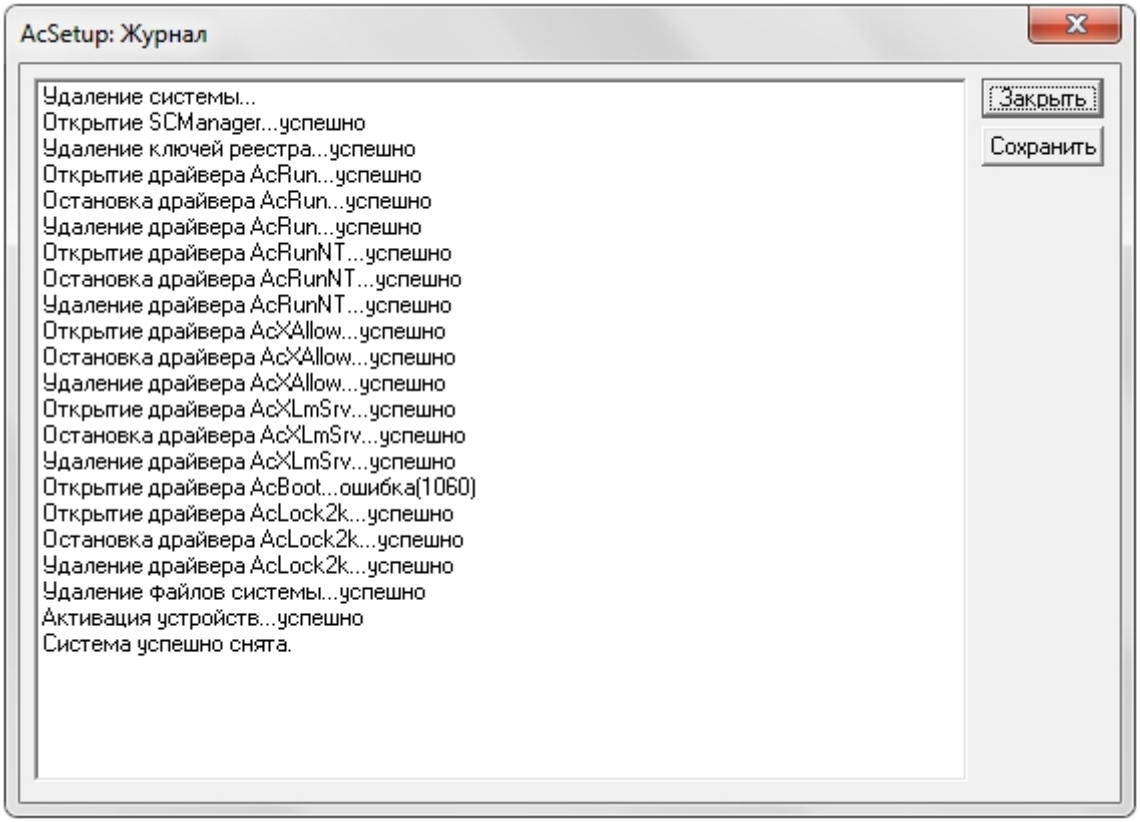


Рисунок 11 – Просмотр журнала команд программы AcSetup.EXE

Команды в журнале AcSetup.EXE можно сохранить (например, для дальнейшего анализа), нажав кнопку <Сохранить> в окне на рисунке 11. При нажатии кнопки на экране появляется окно сохранения файла (рисунок 12), в котором ввести имя файла и нажать кнопку <Сохранить>. Для отмены операции нужно нажать кнопку <Отмена>.

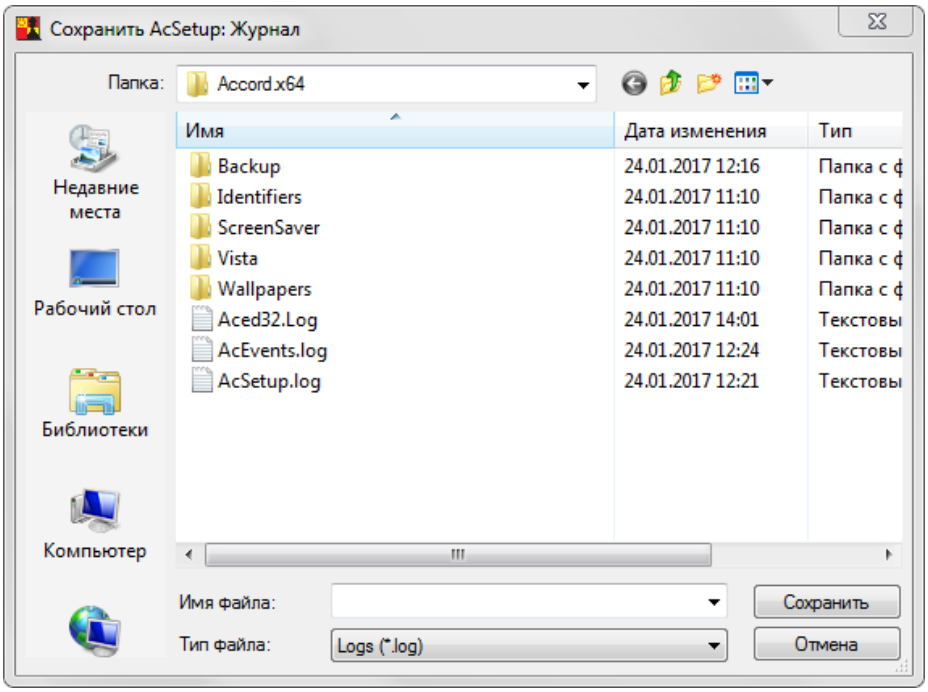


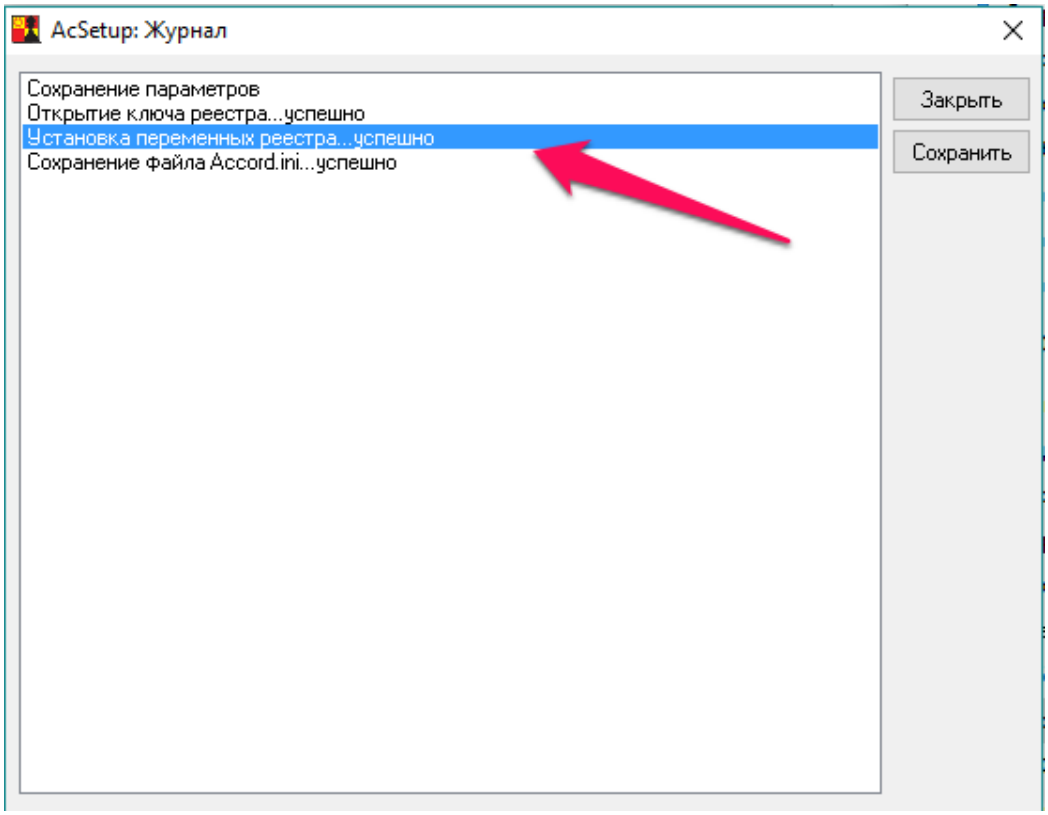
Рисунок 12 – Сохранение журнала программы AcSetup.EXE

2.1.5. Дополнительные параметры настройки СПО «Аккорд»

ВНИМАНИЕ! В утилите AcSetup.exe изменение следующих параметров возможно только при активированном комплексе «Аккорд» (поскольку они прописываются в реестре Windows):

- «Включить подсистему контроля имен общих ресурсов»;
- «Включить подсистему контроля доступа общим ресурсам»;
- «Вести журналы в:»;
- «Изменить экран входа в систему».

Успешное изменение этих параметров можно увидеть в журнале команд, нажав кнопку <Просмотр> в поле «Журнал команд» в главном окне утилиты AcSetup.exe:



При неактивированном комплексе «Аккорд» после изменения параметров и повторного запуска утилиты AcSetup.exe параметры будут иметь значения по умолчанию.

В пункте меню **«Параметры»** главного окна программы настройки СПО «Аккорд» можно изменить дополнительные параметры и настройки СЗИ «Аккорд».

Пункт меню ***«Язык»*** позволяет выбрать язык, на котором будут выводиться сообщения программ, входящих в состав СПО «Аккорд». При старте программы настройки СПО «Аккорд» устанавливается язык, соответствующий основному языку операционной системы. Если у Вас установлена английская версия Windows, то программа начинает работу на английском языке. Если в английской версии ОС установлена поддержка русского языка, то после старта программы в пункте Параметры>Язык можно выбрать «Русский» для вывода сообщений на русском языке.

Пункт меню ***«Категории доступа»*** позволяет редактировать список категорий доступа, который используется в реализации мандатного механизма разграничения доступа (рисунок 13).

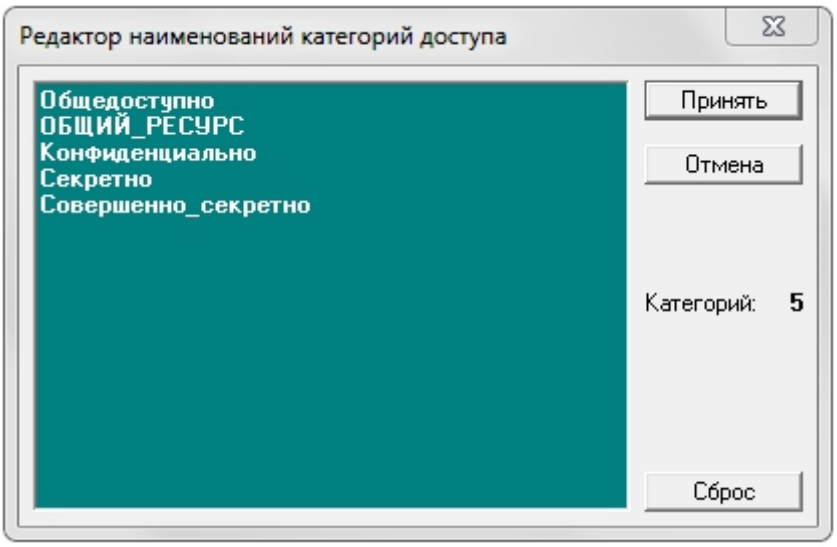


Рисунок 13 - Редактирование списка категорий доступа

При установке СЗИ «Аккорд» в списке уже содержатся пять категорий доступа. Администратор безопасности информации может менять количество и наименование категорий доступа в соответствии с принятой политикой защиты информации. В подсистеме мандатного доступа допускается использование до 15 категорий доступа.

ВНИМАНИЕ! Запрещается переименовывать/удалять категорию доступа «Общий ресурс». Данная категория зарезервирована в СЗИ «Аккорд» как специальная. Начиная с версии 5.0.9.49 ПО СЗИ «Аккорд» по умолчанию не позволяет переименовывать/удалять данную категорию доступа.

Пункт меню ***«Дополнительные опции»*** открывает доступ к настройкам расширенных функций и параметров системы защиты (рисунок 14).

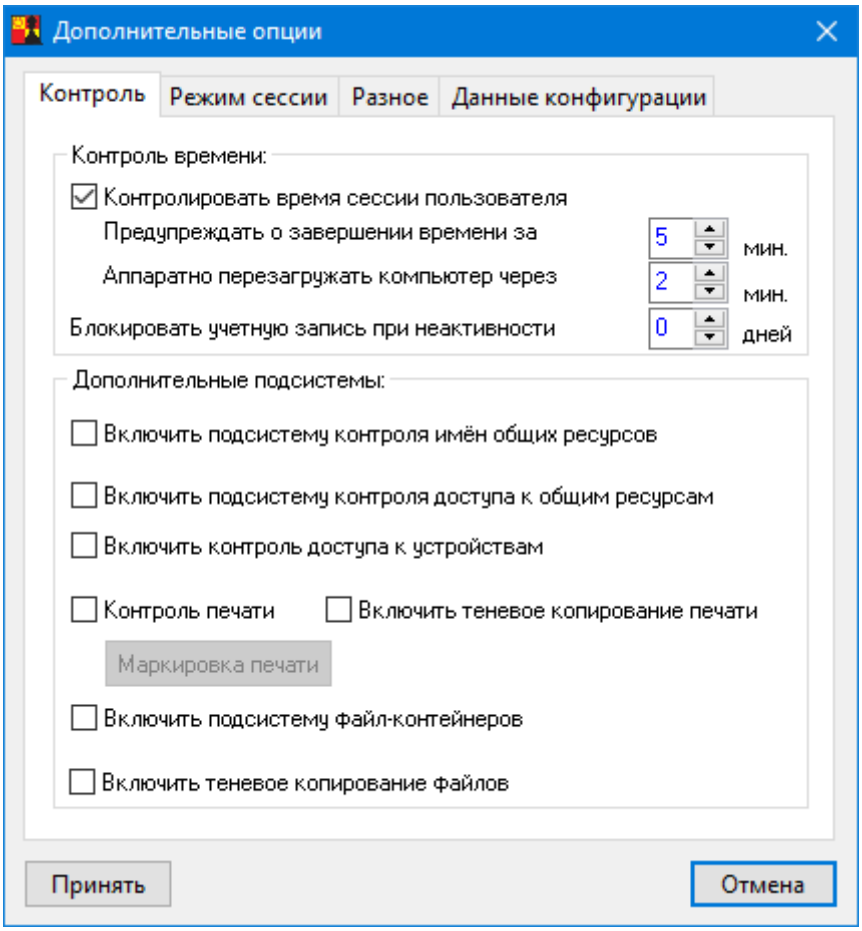


Рисунок 14 - Дополнительные параметры в настройке СЗИ

Дополнительные опции сгруппированы по функциональному назначению и выбираются нажатием левой кнопки мыши на соответствующей закладке.

Закладка **«Контроль»** содержит две группы параметров: «Контроль времени» и «Дополнительные подсистемы».

«Контроль времени» определяет режим принудительного завершения сеанса пользователя, если в редакторе ПРД установлены соответствующие ограничения по времени работы. Если контроль времени включен, то администратор задает интервал (в минутах) до завершения сеанса, когда пользователю выводится предупреждение об окончании работы. Второй параметр – это интервал времени в минутах, по истечении которого аппаратно перезагружается компьютер после попытки выполнить перезагрузку обычным способом. Эта процедура может потребоваться, если какое-либо приложение «зависло» и не отвечает на системные запросы. Параметр «Блокировать учетную запись при неактивности» устанавливает временной период неактивности (в днях), по истечении которого учетная запись пользователя блокируется. Значение сохраняется в файле Accord.ini (параметр InactiveDays).

Группа параметров **«Дополнительные подсистемы»** отвечает за активацию функций СЗИ «Аккорд», которые не относятся непосредственно к разграничению доступа, но определяют режимы работы защищенной рабочей станции в составе сети (автоматизированной системы).

«Включить подсистему контроля имен общих ресурсов» – установка данного параметра активирует (после перезагрузки) процедуру контроля заданных в редакторе ПРД общих ресурсов, т.е. устройств, папок и файлов данного компьютера, предоставленных в общий доступ пользователям сети (подробнее см. документ «Установка правил разграничения доступа. Программа ACED32» пункт «Установка фиксированных сетевых имен ресурсов общего пользования»).

«Включить подсистему контроля доступа к общим ресурсам» – установка данного параметра активирует (после перезагрузки) процедуру контроля доступа к ресурсам данного компьютера из сети. Предыдущий параметр регламентирует выделение ресурсов данного компьютера в общий доступ с фиксированными именами, а данный флаг включает драйвер, который разрешает или запрещает доступ из внешней сети к ресурсам компьютера на время сеанса работы конкретного пользователя. Режим контроля определяется опцией «*Запрет доступа к общим ресурсам*» в настройках пользователя (подробнее см. документ «Установка правил разграничения доступа. Программа ACED32» пункт «Установка дополнительных опций работы пользователя»).

«Включить контроль доступа к устройствам» – установка данного параметра активирует подсистему контроля устройств. После выхода из программы настройки с сохранением данного изменения в программе – редакторе ПРД в списке объектов для установки атрибутов доступа появляется группа «Устройства». Открыв эту группу, администратор получает возможность контроля доступа к любому устройству или классу устройств, доступных в «Диспетчере устройств» Windows, в том числе последовательных и параллельных портов, устройств PCMCI, IEEE 1394, WiFi, Bluetooth и пр. Включение объекта из этой группы в список ПРД означает запрет на доступ к этому объекту, в списке атрибутов доступна только регистрация попыток доступа на чтение или запись.

«Контроль печати» – установка данного параметра активирует подсистему контроля и маркировки печати.

«Включить теневое копирование печати» – установка данного параметра включает процесс теневого копирования информации, выводимой на печать, при котором файлы из очереди печати (.spl) будут скопированы в C:\Accord.x64\!PRN.BKP\UserName\Date Time\.spl.

<Маркировка печати> – данная кнопка предназначена для вызова программы настройки информации, выводимой на маркированный печатный документ. Режим контроля и маркировки печатных документов определяется опцией «*контроль печати*» в настройках опций пользователя (подробнее см. документ «Установка правил разграничения доступа. Программа ACED32» пункт «Установка опций настройки»).

В программе настройки маркировки документов параметры сгруппированы в несколько секций, которые открываются при выборе соответствующей закладки.

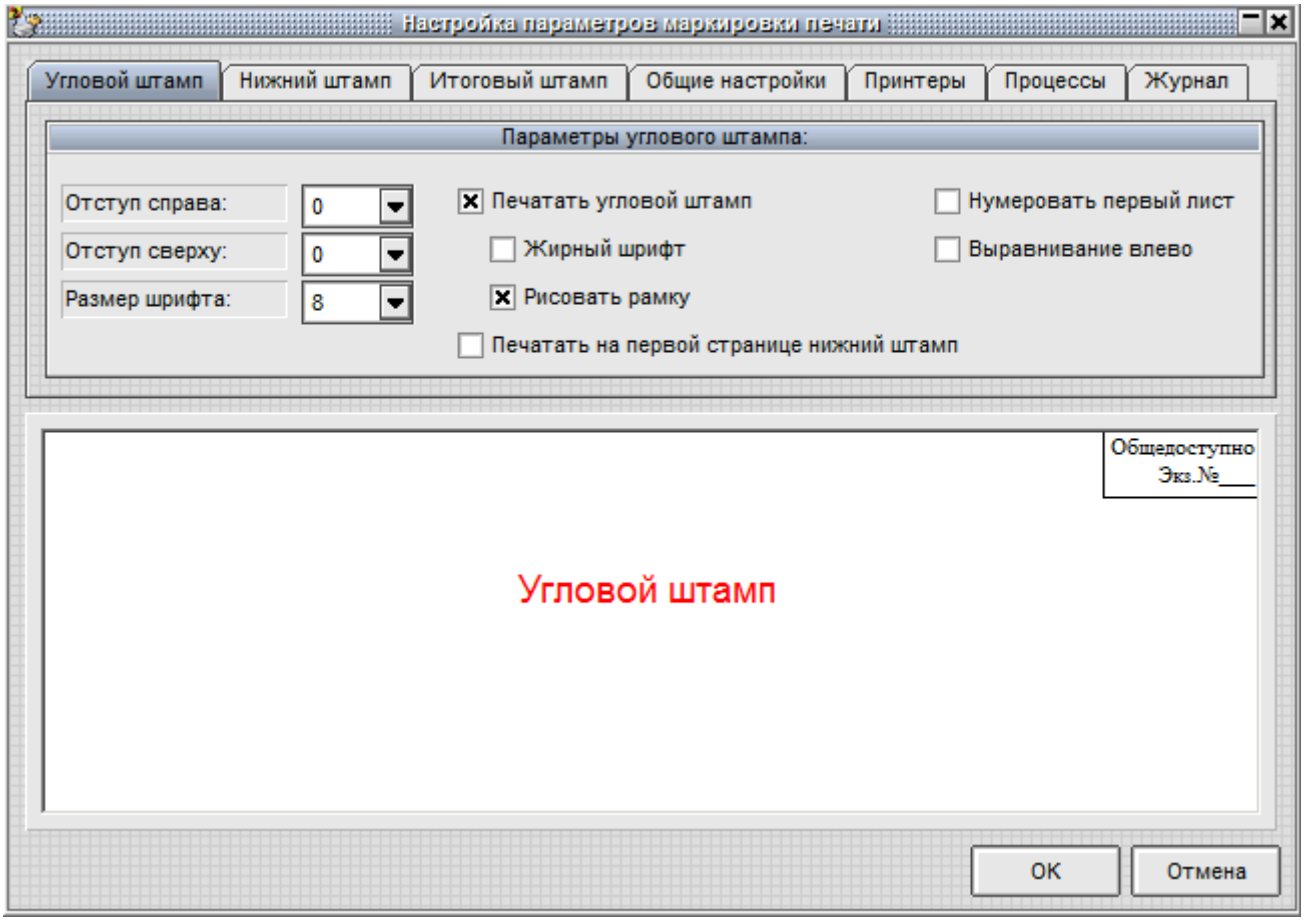


Рисунок 15 - Настройка маркировки первой страницы документа

Закладка **«Угловой штамп»** (рисунок 15) определяет вид информации, выводимой на первой странице маркируемого документа. Параметры «Отступ справа» и «Отступ сверху» определяют положение углового штампа на первой странице. «Размер шрифта» соответствует принятому в ОС Windows типоразмеру шрифтов. Параметры «Жирный шрифт», «Выравнивание влево» и «Рисовать рамку» очевидны и не требуют дополнительной детализации. Параметр «Печатать на первой странице нижний штамп» определяет способ маркировки, когда на первой странице кроме верхнего углового штампа печатается еще информация нижнего колонтитула, которая выводится на всех страницах документа, но в отдельных случаях не требуется именно на первой странице. Параметр «Нумеровать первый лист» показывает, будет ли печататься на первом листе номер страницы.

Закладка **«Нижний штамп»** (рисунок 16) определяет вид информации, выводимой в нижней части страницы маркируемого документа.

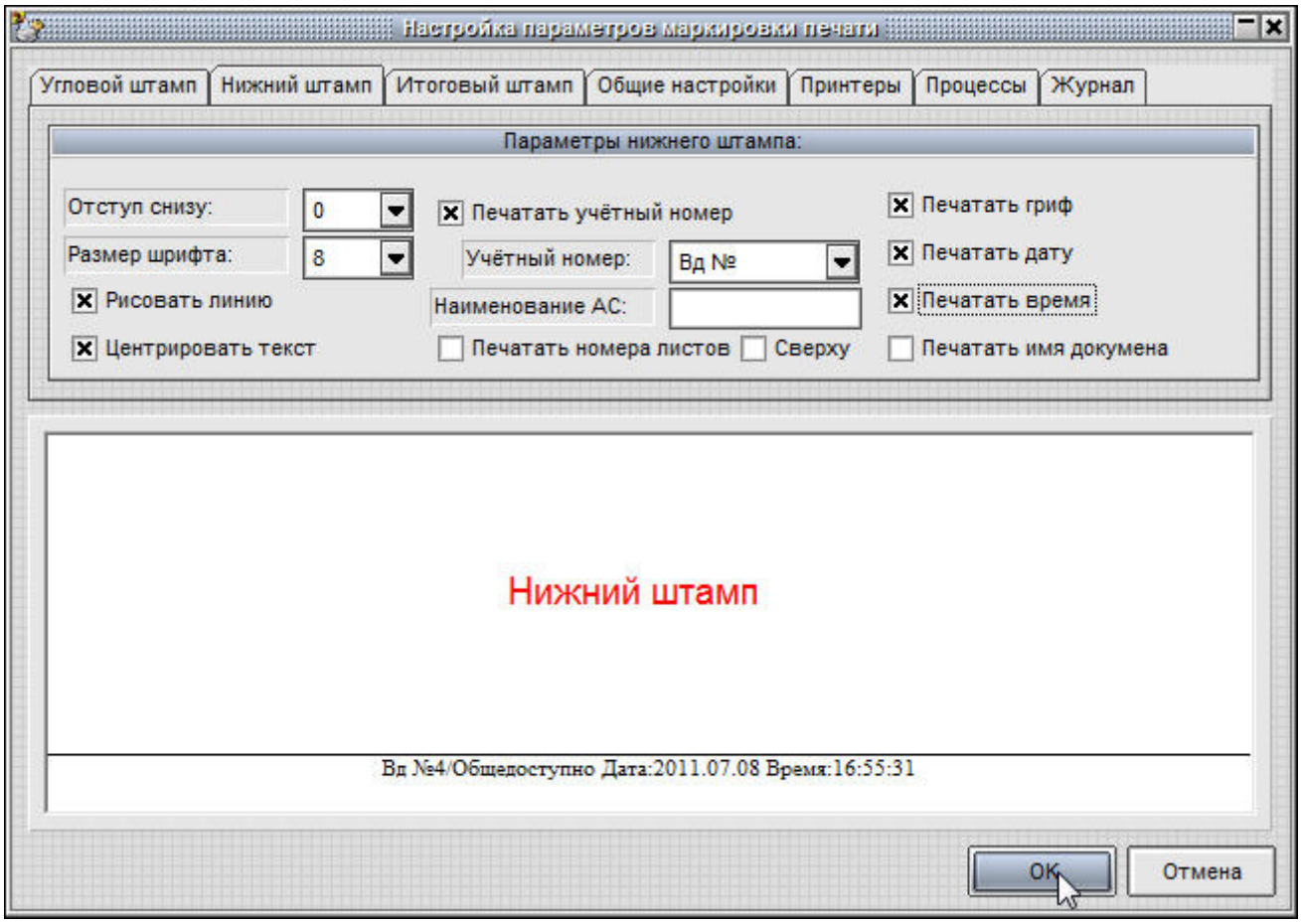


Рисунок 16 - Настройка нижнего колонтитула маркированного документа

Параметры «Отступ снизу» и «Размер шрифта» задают положение на странице и размер шрифта маркирующей информации. Флаг «Рисовать линию» включает «отбивку» нижнего штампа линией, а флаг «Центрировать текст» определяет положение на странице. Флаги в правой части окна определяют, какую информацию печатать в нижнем штампе. Отдельного разъяснения требует флаг **«Печатать гриф»** - это информация о грифе конфиденциальности документа. Корректно определить гриф при выводе на печать можно только при включенном механизме мандатного контроля доступа. Если используется мандатный механизм без контроля процессов, то гриф определяется меткой доступа редактируемого объекта[4]. Если используется мандатный механизм с контролем процессов, то гриф определяется уровнем доступа процесса, открывшего документ. В процедуре управления потоками информации нельзя бесконтрольно понижать гриф, а для процесса с высоким уровнем секретности доступны на чтение все объекты с метками нижестоящего уровня. Система защиты исключает вариант, когда программа открывает общедоступный файл, добавляет в него секретные сведения и отправляет на

[4] Если в процессе работы с документами разных грифов конфиденциальности вывести на печать документ с высоким грифом, а затем документ с низким грифом конфиденциальности, то последний документ в процессе печати получит высокий гриф конфиденциальности. Для печати документа с низким грифом конфиденциальности следует закрыть все документы и открыть для печати только документ с низким грифом

печать без грифа секретности. Если такой механизм маркировки грифа не подходит по регламенту, то администратор может в общих настройках маркировки включить флаг «Гриф указывается пользователем», и эта информация будет вводиться пользователем в экранной форме, которая появляется перед печатью документа. «Учетный номер» не может определяться автоматически, поэтому значение этого параметра пользователь также вводит вручную. Если в поле «Наименование АС» администратор вводит текстовую информацию, то эти данные будут автоматически выводиться при маркировке документа. Флаг «Печатать номера листов» определяет, будут ли печататься номера листов. Флаг «Сверху» переводит печать нижнего штампа в верхнюю часть страницы.

Закладка **«Итоговый штамп»** (рисунок 17) определяет вид информации, выводимой на последней странице документа. По требованиям делопроизводства эта информация печатается на оборотной стороне последней страницы. Флаг «Выводить предупреждение о печати последнего листа» требуется включить, если принтер не оборудован устройством подачи бумаги для двусторонней печати. В таком варианте печать последней страницы выполняется после подтверждения пользователя, и можно вручную перевернуть страницу.

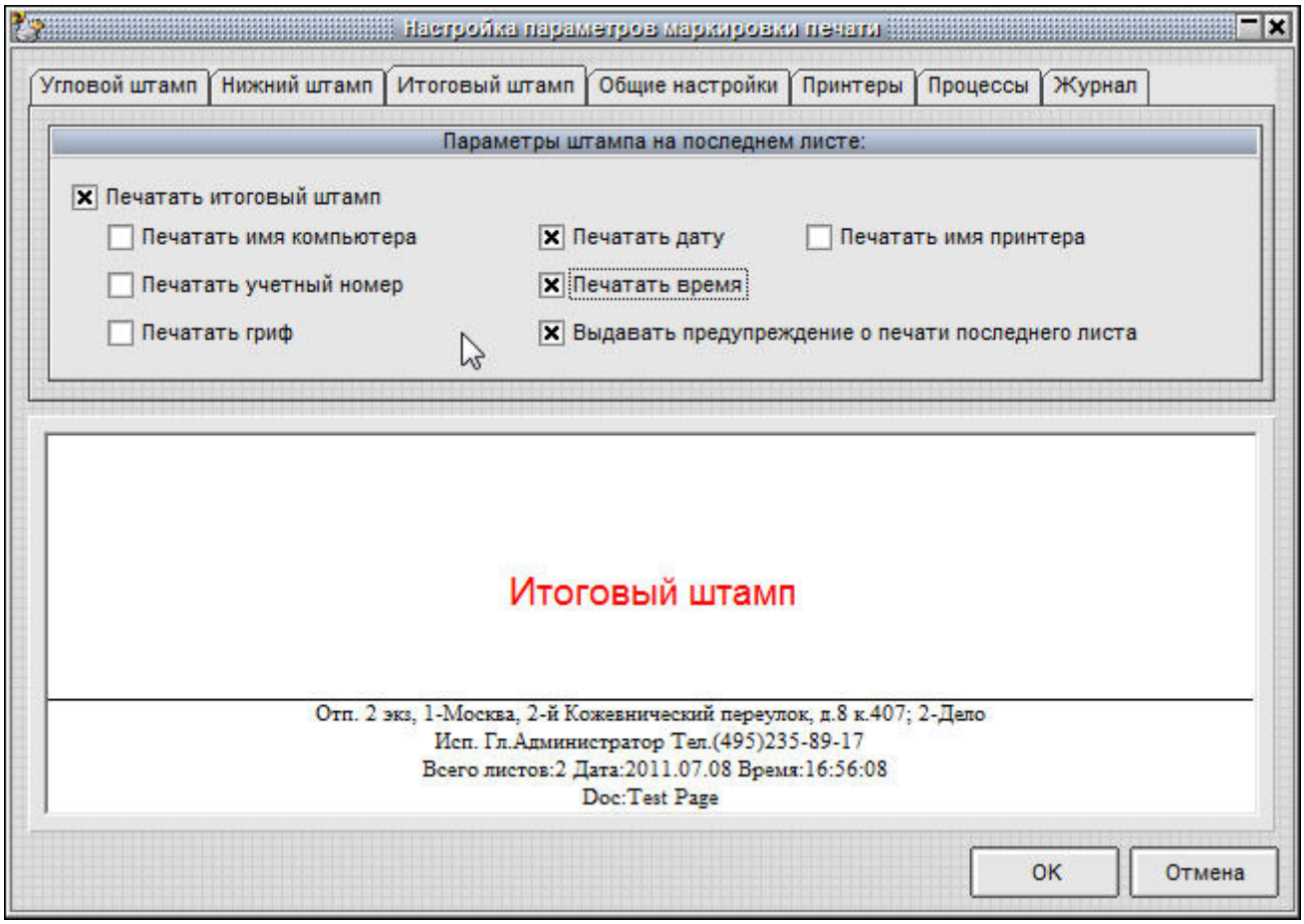


Рисунок 17 - Настройка маркировки последней страницы документа

Закладка **«Общие настройки»** (рисунок 18) определяет режимы работы подсистемы контроля печати. Администратор может выбрать уровень

конфиденциальности документов, начиная с которого выполняется маркировка, возможность ручного ввода грифа и названия документа, фамилии пользователя и общего количества печатных листов. Если администратор запрещает ручной ввод ФИО пользователя, то документ маркируется полным именем из базы данных СЗИ «Аккорд», а если это поле не заполнено, то коротким. В журнал регистрации печати всегда выводится имя из базы данных, даже если разрешен ручной ввод этого параметра. «Регистрационный номер машинного носителя» - это текстовое поле, которое выводится на последней странице печатного документа по требованию регламента некоторых организаций.

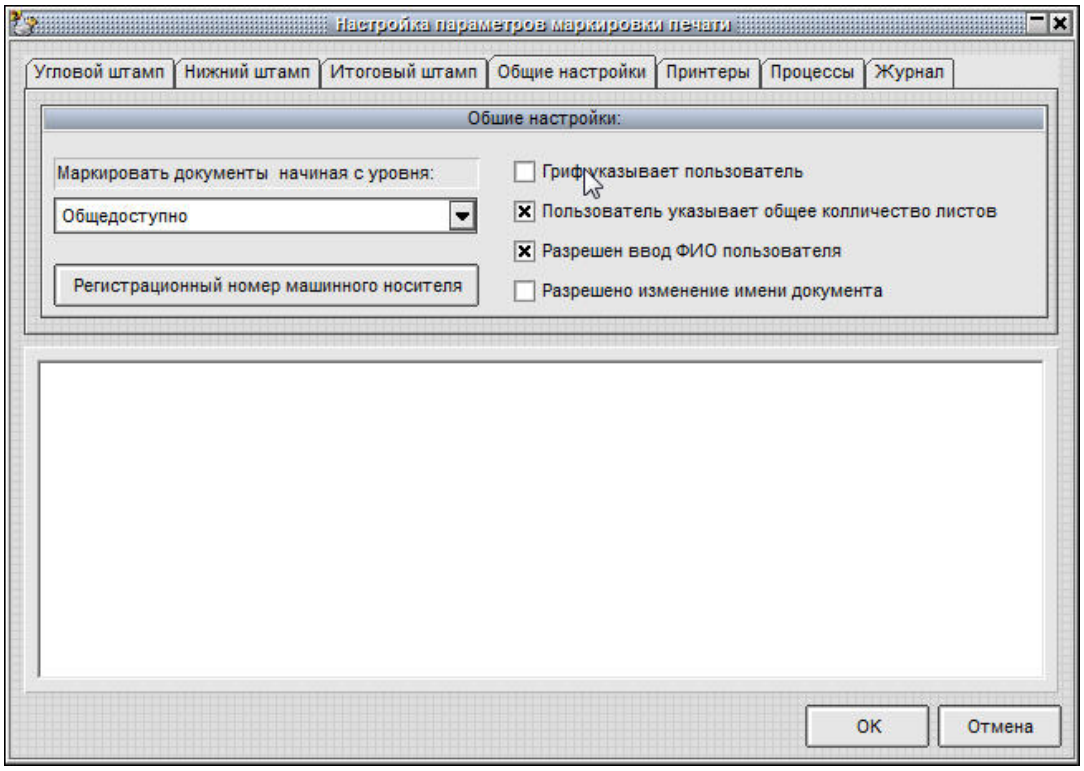


Рисунок 18 - Общие настройки режима маркировки

Закладка **«Принтеры»** (рисунок 19) позволяет администратору исключить отдельные печатающие устройства из процесса маркировки документов. Например, устройство PDF Complete – это виртуальный принтер, и вывод осуществляется в файл. Вполне возможно, что в таком варианте маркировка не потребуется.

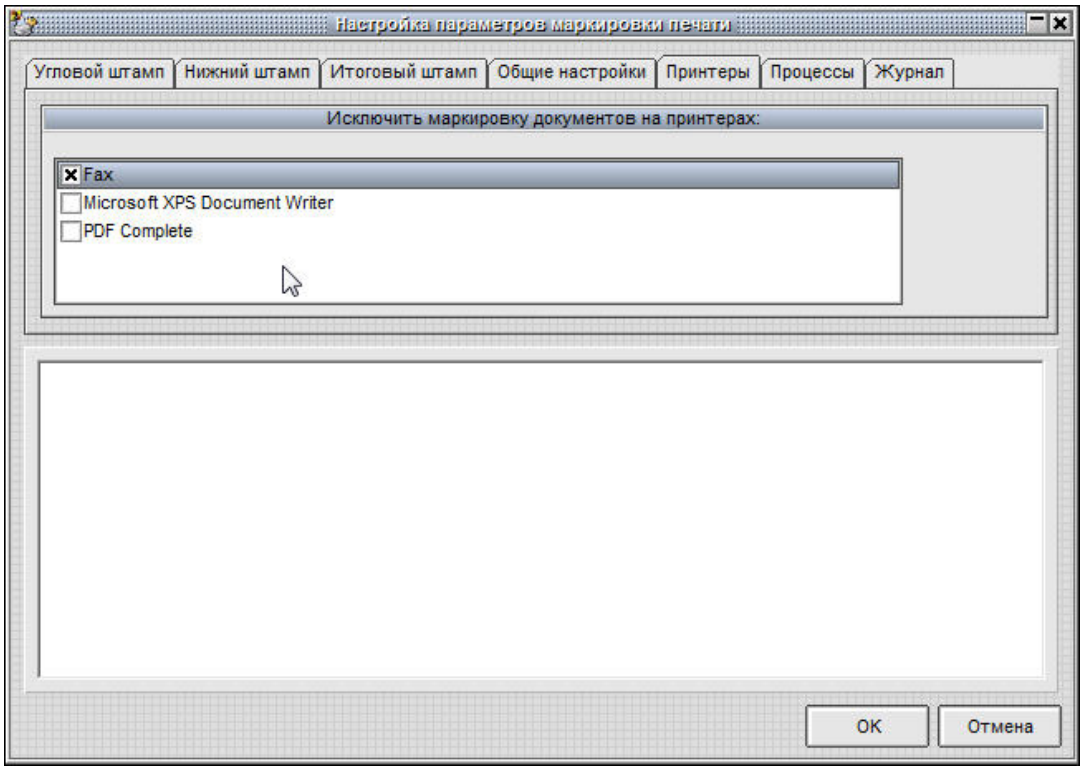


Рисунок 19 - Выбор исключений печатающих устройств

Закладка **«Процессы»** позволяет администратору сформировать список процессов, для которых маркировка документов средствами СЗИ «Аккорд» выполняться не будет. Такой режим пригодится в том случае, когда прикладное ПО самостоятельно формирует маркировочную информацию в документах, выводимых на печать. Если не сформировать список исключений, то документ будет маркироваться дважды.

Выбор закладки **«Журнал»** открывает режим просмотра журнала регистрации событий вывода на печать. В журнале документы, которые выводились без маркировки, отображаются черным шрифтом, с маркировкой – синим, а красным шрифтом отображаются события, которые завершились с кодом ошибки (рисунок 20).

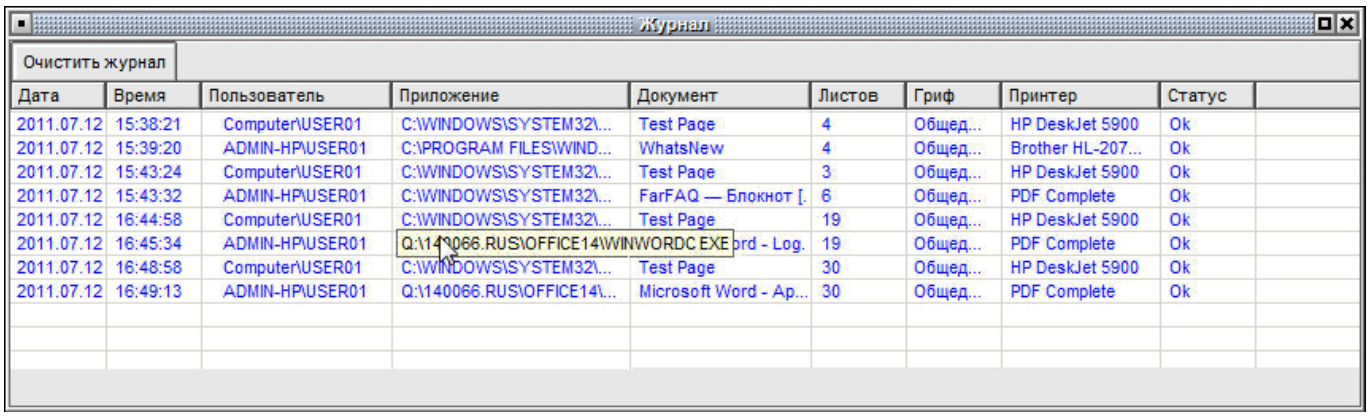


Рисунок 20 - Журнал регистрации вывода на печать

Имеется возможность очистки журнала регистрации событий. Перед выполнением процедуры очистки информацию, хранящуюся в журнале, можно сохранить, поместив в архив. Для этого необходимо нажать кнопку <Очистить журнал> (рисунок 20).

На рисунке 21 приведена форма, которая выводится на экран перед отправкой документа на печать, если для данного пользователя включен режим маркировки.

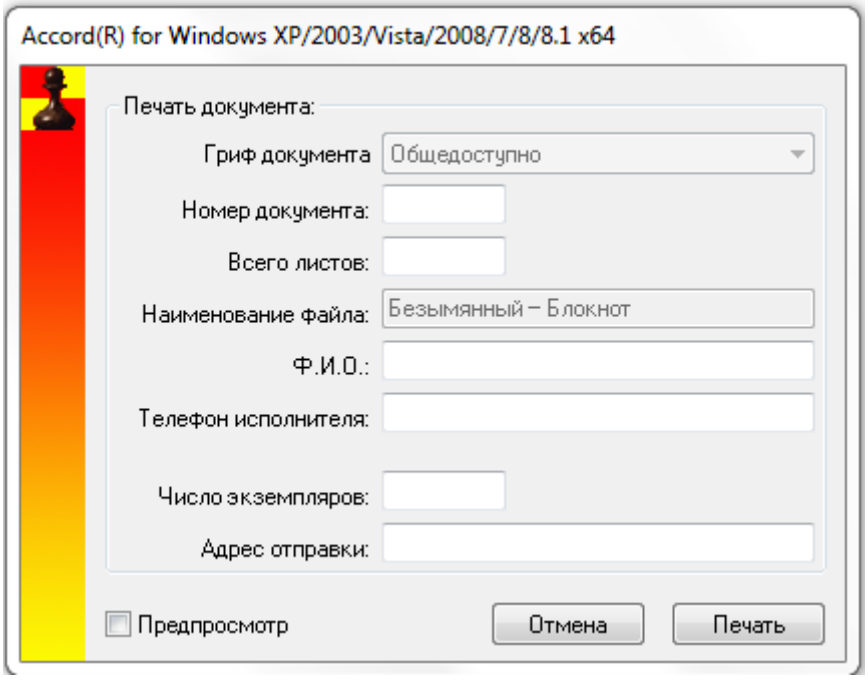


Рисунок 21 - Окно ввода дополнительных полей маркировки документа

ВАЖНО! В случае если печать документа, требующего маркировки, будет осуществляться в файл с использованием виртуального принтера, форма вывода на печать «Последний лист» будет постоянно повторяться ввиду отсутствия обратного ответа от виртуального принтера. После печати последнего листа при повторном выводе формы «Последний лист» нажмите кнопку <Отмена>.

Часть полей обязательна для ввода, часть задается администратором в настройках. Если пользователь не заполнил одну или несколько строк обязательной информации, то печать документа не выполняется, а в открытом окне курсор мигает в той строке, которую требуется ввести.

После закрытия окна «Маркировка печати» программа возвращается к настройкам режимов работы СПО «Аккорд».

«Включить подсистему файл-контейнеров» – установка данного параметра позволяет активировать подсистему работы с файл-контейнерами. Активация подсистемы происходит после перезагрузки СВТ, когда в трее появляется иконка  . По клику на ней правой кнопкой мыши открывается меню подсистемы (рисунок 22).

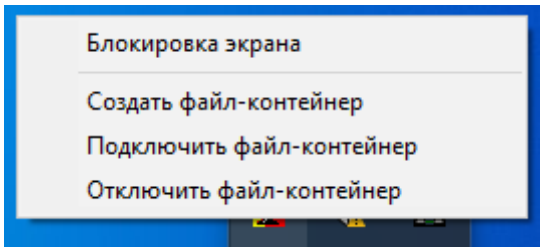


Рисунок 22 - Меню подсистемы файл-контейнеров

При выборе в этом меню команды **«Создать файл-контейнер»** появляется окно (рисунок 23), в котором следует указать путь к образу файл-контейнера, размер диска, выбрать файловую систему (FAT32 или NTFS) и букву монтируемого диска. Путь к файлу образа выбирается по кнопке <Обзор>. Файл может быть расположен на жестком диске, на сетевом диске и на съемном носителе. Не рекомендуется указывать корневой каталог диска С.

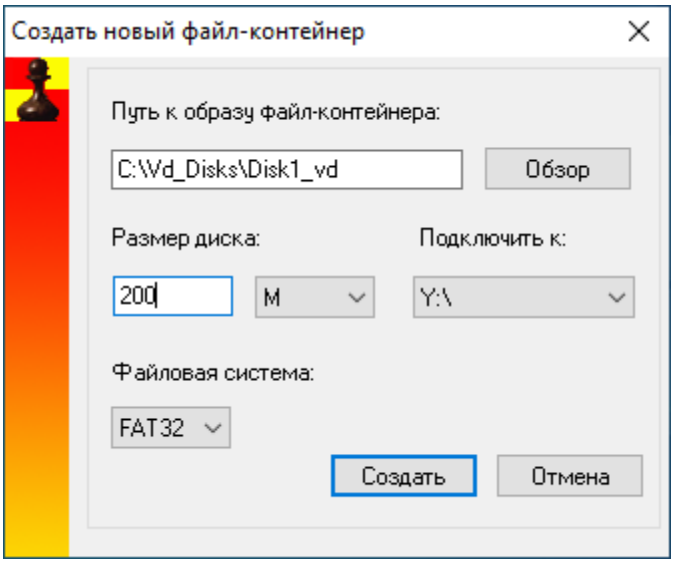


Рисунок 23 - Создание файл-контейнера

После заполнения полей с параметрами файл-контейнера следует нажать кнопку <Создать>, далее по запросу предъявить идентификатор пользователя. О том, что файл создан и отформатирован, будет свидетельствовать появление соответствующего сообщения (рисунок 24).

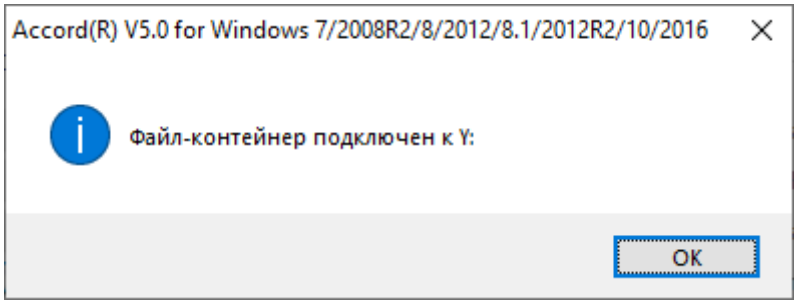


Рисунок 24 - Подтверждение создания файл-контейнера

Созданный файл можно отключить при выборе в меню (рисунок 22) команды **«Отключить файл-контейнер»**. Выполнение данной команды сопровождается соответствующим оповещением (рисунок 25).

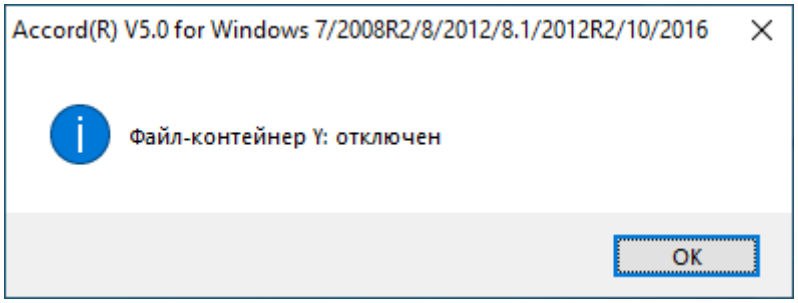


Рисунок 25 - Подтверждение отключения файл-контейнера

При необходимости подключить файл-контейнер следует выбрать команду **«Подключить файл-контейнер»**. В появившемся окне (рисунок 26) можно выбрать путь к образу файл-контейнера и назначить букву для подключения.

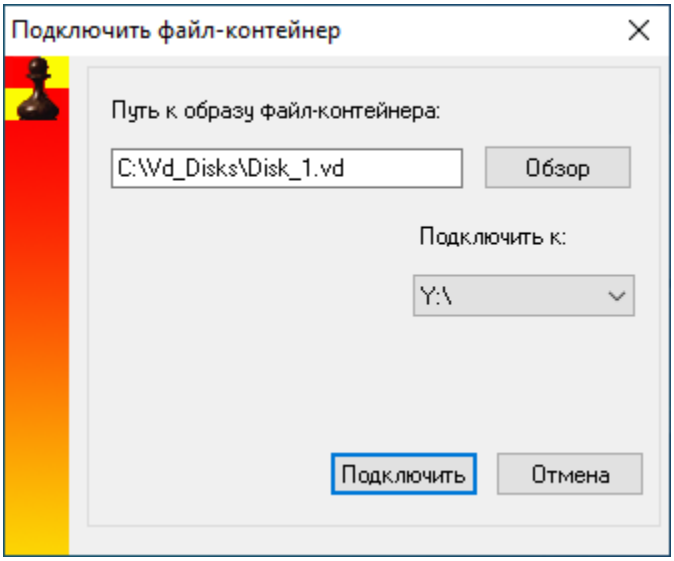


Рисунок 26 - Подключение файла-контейнера

Далее нажать кнопку <Подключить> и по запросу предъявить идентификатор пользователя. При успешном подключении появляется сообщение, отображенное на рисунке 24.

«Включить теневое копирование файлов» – установка данного параметра включает процесс теневого копирования файлов при отчуждении их на съемный носитель.

Закладка **«Режим сессии»** определяет процедуры начала и завершения работы монитора системы безопасности ACRUN.SYS (рисунок 27).

ВНИМАНИЕ! Для вступления в силу изменений параметров, выполненных в закладке «Режим сессии», необходима перезагрузка СВТ.

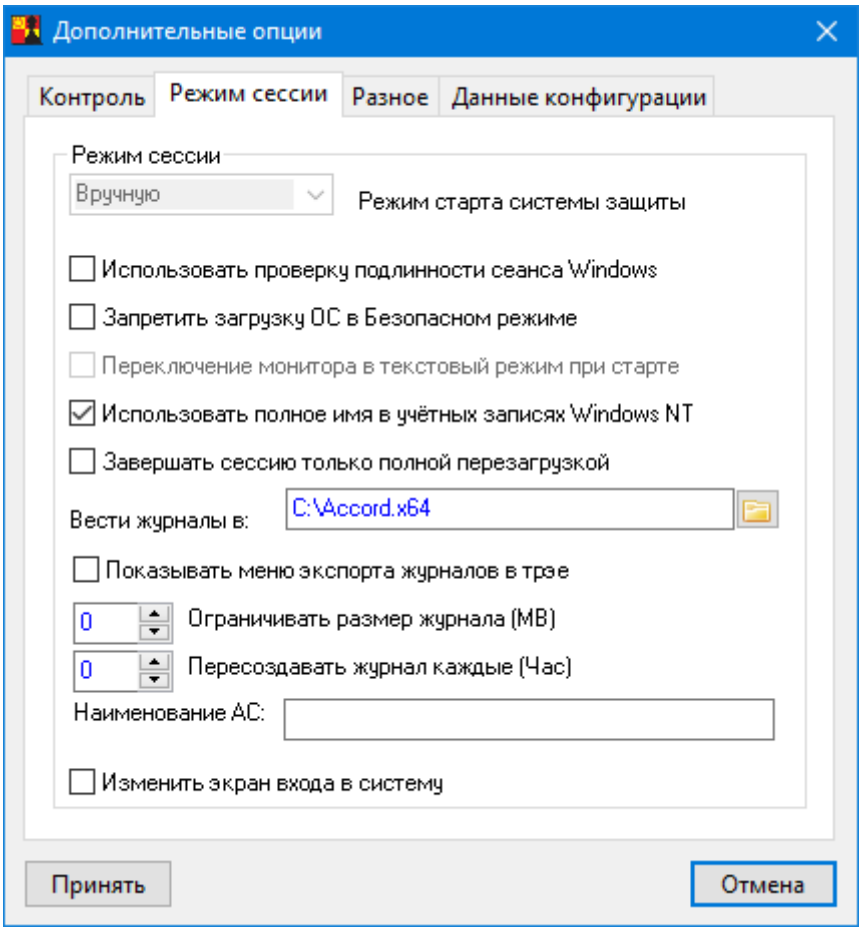


Рисунок 27 - Дополнительные параметры «Режим сессии» в настройке СЗИ

«Режим старта системы защиты» – определяет вариант загрузки монитора безопасности. В СПО «Аккорд-Win64 K» режим старта системы защиты «Вручную» установлен по умолчанию (опцию изменить нельзя). Режим «Вручную» определяет, что монитор безопасности стартует позже, и подключает правила доступа на основании информации, полученной от модуля AcGina.DLL.

«Использовать проверку подлинности сеанса Windows» - при установке этого флага авторизация пользователя выполняется средствами провайдеров Windows. «Аккорд-Win64» получает учетные данные пользователя ОС, запрашивает идентификатор и получает полное имя пользователя из базы «Аккорд-Win64». В случае, если и в учетных данных пользователя для входа в систему, и в полном имени пользователя в базе СПО «Аккорд-Win64» указано доменное имя, проводится дополнительная проверка на совпадение имен и доменов пользователя в ОС и в базе «Аккорд-Win64».

Флаг ***«Запретить загрузку ОС в Безопасном режиме»*** блокирует возможность выбора старта ОС в безопасном режиме, т.к. этот режим позволяет не загружать отдельные драйверы и запускает стандартную процедуру WinLogOn, которая не предусматривает дополнительной идентификации пользователя, тем самым допускает «обход» модулей СЗИ. В режимах старта СЗИ «Загрузка» и «Система» этой опасности нет, т.к. монитор безопасности грузится на уровне ядра системы, и его обход невозможен в любом варианте загрузки ОС. Этот флаг устанавливается в том случае, когда выбран режим

старта «Вручную» или когда администратор безопасности хочет исключить возможность загрузки системы в обход процедуры WinLogOn. Включать этот флаг следует только после окончательной настройки работы компьютера в защищенном режиме.

ВНИМАНИЕ! Опция «Запретить загрузку ОС в Безопасном режиме» работает только при выключенной опции «Перезагрузка при ошибках» (см. п. 2.1.4).

«Переключение монитора в текстовый режим при старте»[5] установлен по умолчанию. Если отключить этот флаг, то информация о старте монитора безопасности будет выводиться в графическом режиме, но только по-английски, т.к. на этапе загрузки ядра ОС еще нет поддержки MUI и возможности выбора графических шрифтов.

«Использовать полное имя в учетных записях Windows NT» – при установке этого параметра имя пользователя, заданное в редакторе ПРД ACED32 в поле «Полное имя», будет использоваться при синхронизации с базой учетных записей ОС. Такой режим необходим в том случае, когда пользователь подключается к контроллеру домена, который использует «длинные» имена.

«Завершать сессию только полной перезагрузкой»[6] – при установке этого параметра после завершения сеанса пользователя выполняется принудительная перезагрузка компьютера, т.е. нельзя завершить сеанс работы одного пользователя и начать другой без перезагрузки компьютера.

Старт модуля ACRUN.SYS в режиме загрузочного драйвера и завершение сессии перезагрузкой могут понадобиться, например, при включении драйверов сетевой карты в список запрещенных (скрытых) файлов. В таком варианте пользователь (и любая системная или прикладная программа) не получит доступа к сетевым ресурсам, но восстановление подключения к сети для другого пользователя возможно после полной перезагрузки.

При нажатии на раскрывающийся список в поле ***«Вести журналы в:»*** можно выбрать каталог, в который сохраняются файлы журнала событий СПО «Аккорд-Win64 K».

«Показывать меню экспорта журналов в трэе» – при установке этого параметра при нажатии правой кнопкой мыши на иконку СПО «Аккорд» в трэе на экране появляется меню, в котором отображаются два флага: «Блокировать экран», «Экспортировать журналы». Выбор первого флага приведет к запуску хранителя экрана. Посредством выбора второго флага можно экспортировать журналы на внешний носитель. Экспорт журналов может осуществлять только пользователь группы «Администраторы» с установленной привилегией «Управление журналом». После выполнения команды экспорта происходит закрытие текущего журнала и создание нового, в который записывается информация о пользователе, который экспортировал журналы (информация о пользователе также записывается в журнал событий входа в ОС Windows AcEvents.log, содержащий сведения о дате, времени и результате выполнения операции входа в ОС Windows с указанием идентификатора и имени

---

[5] В ОС Windows Vista и выше флаг «Переключение монитора в текстовый режим при старте» блокируется

[6] В терминальной версии СПО «Аккорд-Win64 K» флаг «Завершать сессию только полной перезагрузкой» отсутствует

пользователя - подробнее о формате журнала см. Приложение 1). Чтобы изменение положения флага вступило в силу, необходимо выполнить перезагрузку СВТ, на котором установлено СПО «Аккорд».

«Ограничивать размер журнала (МВ)» - параметр позволяет разбивать журналы событий по указанному размеру. Любое значение, отличное от нуля, будет указывать на размер файла журнала (*.low), при достижении которого журнал автоматически закроется, и будет создан новый файл.

«Пересоздавать журнал каждые (Час)» - значение (отличное от нуля), указанное в этой строке, устанавливает время, по истечении которого журнал событий автоматически закроется, и будет создан новый файл журнала (*.low). Значение сохраняется в файле Accord.ini (параметр LogTime).

В закладке «Режим сессии» также можно указать каталог, в котором находится журнал, и установить имя АС.

В СПО «Аккорд-Win64 K» имеется возможность задания уникального имени для СВТ. Для этого в поле **«Наименование АС»** следует вручную ввести имя АС. Имя АС отображается в журнале событий СПО «Аккорд-Win64 K» (файлах типа *.low).

«Изменить экран входа в систему» - этот параметр позволяет изменить фон диалогового окна входа в систему[7].

Закладка **«Разное»** содержит ряд дополнительных параметров, влияющих на режим функционирования СЗИ (рисунок 28).

Первые три параметра относятся к дисциплине гарантированного удаления остаточной информации, которая включается флагом «Удаление файлов с очисткой» в дополнительных опциях пользователя. (При удалении файлы сразу очищаются в корзине).

«Число проходов при очистке файлов» – этим параметром задается количество циклов заполнения случайными данными области на жестком диске, занимаемой удаляемым файлом.

«Очищать файлы, начиная с уровня» - параметр работает при включенном механизме мандатного доступа, когда требуется очищать остаточную информацию для файлов с определенного уровня конфиденциальности.

«Очищать файл подкачки» – включение этого параметра означает, что файл подкачки (виртуальная память ОС) будет очищен при завершении сеанса работы пользователя.

[7)] Для ОС Vista и ниже в программе «Настройка комплекса Аккорд» флаг «Изменить экран входа в систему» отсутствует.

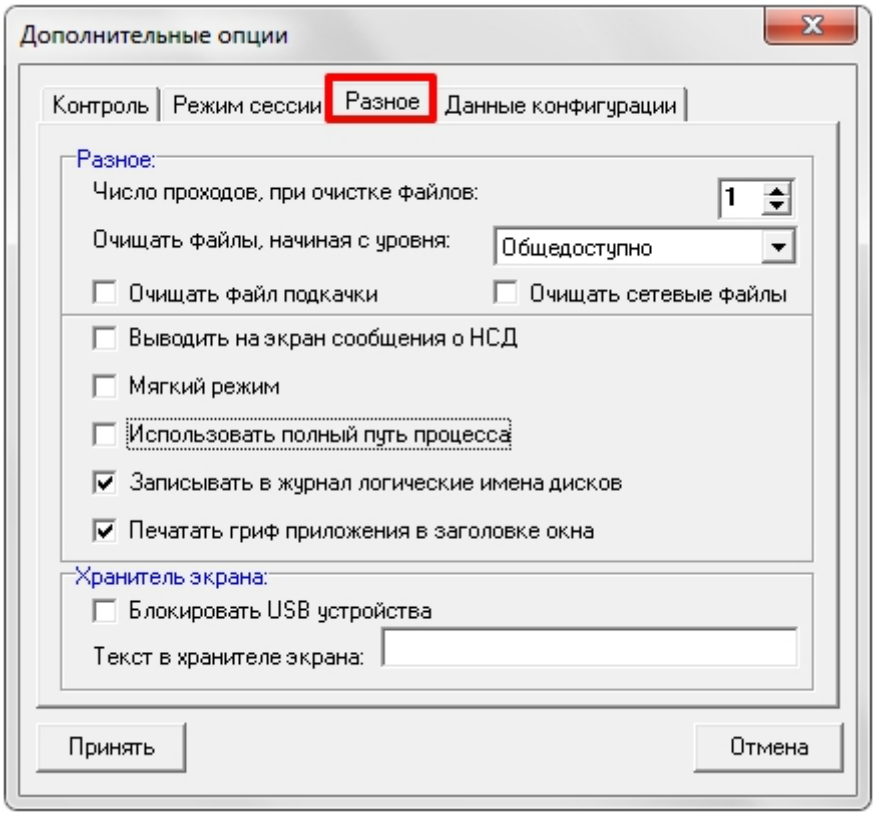


Рисунок 28 - Дополнительные параметры «Разное» в настройке СЗИ

Остальные параметры определяют различные дополнительные режимы работы СЗИ.

«Выводить на экран сообщения о НСД» - включение этого параметра означает, что сообщения об НСД будут выводиться сначала от имени СЗИ «Аккорд», а потом будут дублироваться отказами системы. Этот режим может понадобиться на период настройки и отладки политики безопасности, чтобы понять, какие ограничения накладываются СЗИ, а какие – настройками политик ОС. В обычном режиме СЗИ «Аккорд» генерирует код ошибки, передает его системным службам, и все отказы в доступе выводятся на уровне стандартного интерфейса ОС.

«Мягкий режим» – установка этого параметра позволяет собирать статистику о ресурсах, которые необходимы для работы прикладного ПО и операционной системы. В этом режиме при обращении к запрещенному (недоступному) ресурсу системой «Аккорд» выводится сообщение об НСД, если включен соответствующий параметр (см. предыдущий пункт), попытка НСД заносится в журнал регистрации событий, но выполнение операции не прерывается. Использование этого режима допускается только на период отладки системы защиты и сбора статистики.

Для удобства администратора значение данного параметра («Включен» или «Выключен») отображается в главном окне программы настройки комплекса «Аккорд» (группа элементов «Состояние»).

ВНИМАНИЕ! Для вступления в силу изменения параметра «Мягкий режим» необходима перезагрузка СВТ.

«Использовать полный путь процесса» – этот параметр определяет варианты проверки пути доступа при вызове или контроле процессов. По умолчанию этот флаг не установлен и процесс в файле настроек ПРД описывается только по имени. Включение данного параметра означает, что проверка будет осуществляться по полному пути, т.е. \устройство\том\каталог\файл. Такой режим проверки более строгий.

«Записывать в журнал логические имена дисков» – этот параметр определяет форму записи в журнал регистрации событий. В NT-подобных версиях Windows логические разделы жесткого диска представляются в виде устройство\том\, например, DEVICE\HardDisk0\Volume\. Включение данного параметра позволяет вести запись журнала в формате Лог.устройство:\каталог\файл, например, C:\WINNT\TEMP. После начальной установки СЗИ «Аккорд» этот флаг включен.

«Печатать гриф приложения в заголовке окна» - параметр относится к работе процессов с разными уровнями доступа. При включенном параметре в заголовке окна приложения выводится текущий уровень доступа процесса. В каждый момент пользователь имеет информацию о полномочиях работающего приложения.

Панель **«Хранитель экрана»** содержит только один параметр

«Блокировать USB устройства» – этот параметр позволяет отключать USB порты на время работы хранителя экрана. В обычном режиме, когда порты остаются включенными, появление нового USB устройства снимает Screen Saver и выводит на экран стандартное сообщение о подключении нового устройства. При работе на защищенных СВТ с конфиденциальной информацией такой режим обычно противоречит политике безопасности, поэтому данный параметр должен быть включен администратором. Выключение этого параметра может потребоваться в случаях:

- когда к компьютеру через USB-порт подключен принтер (или другое устройство), который выделен в общий доступ для других пользователей в сети. При такой конфигурации включение хранителя экрана и блокировка USB отключают доступ к устройству другим пользователям.
- когда в качестве персональных идентификаторов используются USB-идентификаторы (ТМ-идентификаторы с USB-считывателем, USB-устройство ШИПКА). При включенном флаге после включения хранителя экрана происходит блокировка USB-идентификаторов, разблокировать компьютер можно только перезагрузив его.

При выборе флага «Блокировать USB устройства» на экране появляется сообщение о блокировке выхода из Хранителя экрана, если используемые пользователем идентификаторы подключены к USB-порту СВТ.

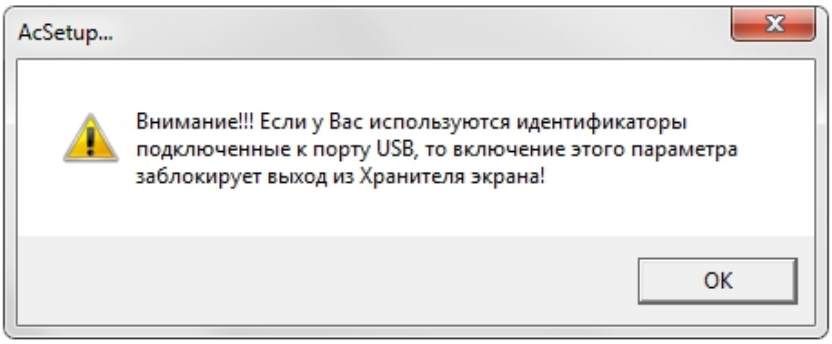


Рисунок 29 – Сообщение о блокировке выхода из Хранителя экрана

ВНИМАНИЕ! Редактирование параметров «хранителя экрана» выполняется с помощью программы-редактора ПРД.

«Текст в хранителе экрана» – Строка символов, которая отображается на экране в момент работы ScreenSaver Аккорд.

Закладка **«Данные конфигурации»** содержит параметры, позволяющие менять интервалы времени для идентификации и ввода пароля (рисунок 30).

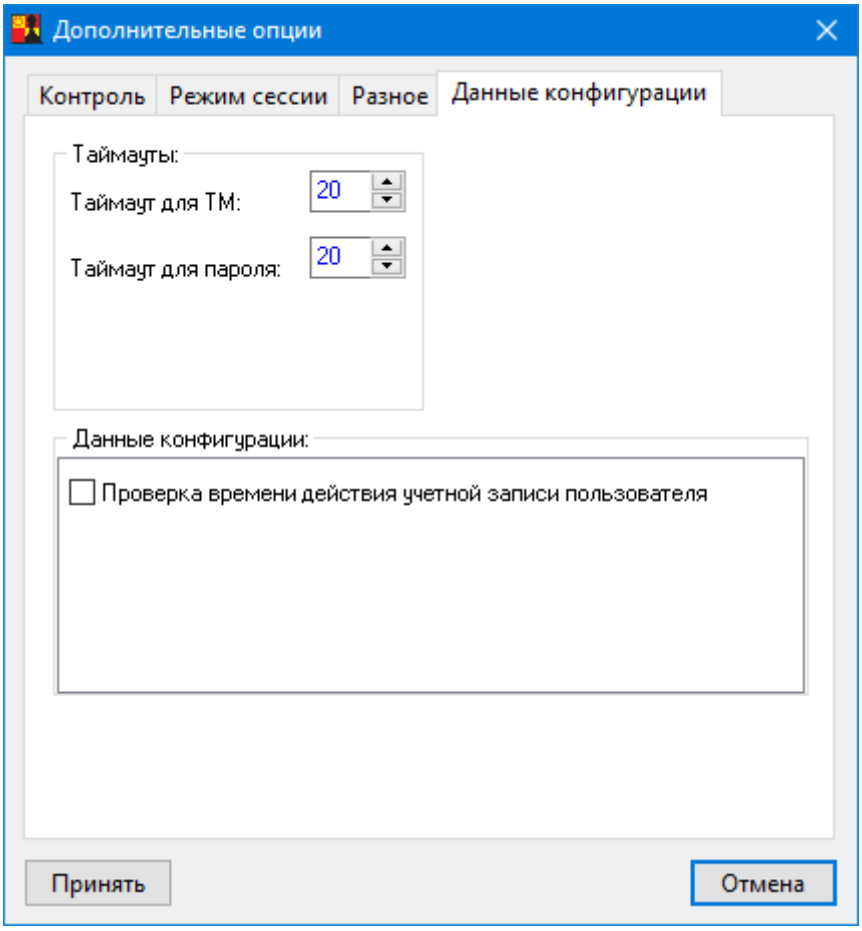


Рисунок 30 - Закладка «Данные конфигурации»

2.1.6. Особенности настройки СПО «Аккорд» при использовании SATA жестких дисков, или RAID контроллеров с динамическим подключением томов

В современных компьютерах все чаще используются жесткие диски, подключаемые по интерфейсу SATA. При этом на материнских платах используются встроенные RAID контроллеры. Логические тома жесткого диска в такой конфигурации могут подключаться динамически. Поскольку монитор разграничения доступа AcRun.SYS стартует на самом раннем этапе загрузки (практически вся загрузка ОС выполняется под его контролем), могут возникнуть трудности с определением соответствия логических имен разделов жесткого диска и их полных системных имен. Такая же проблема может возникнуть при использовании съемных жестких дисков.

Если в редакторе ПРД в списке объектов доступа файл отображается не в привычном виде, например, C:\TMP\my_file.txt, а, к примеру, таким образом:

\DEVICE\HARDDISKDMVOLUMES\EDSRV01DG0\VOLUME1\TMP\my_file.txt,

то у Вас именно такой случай. Для успешной работы СПО «Аккорд» нужно предпринять следующие действия:

1. Закрыть редактор ПРД без сохранения изменений.
2. Удалить файл C:\ACCORD.x64\accord.amz (C:\ACCORD.NT\accord.amz – для 32-битных ОС).
3. В файле C:\ACCORD.x64\accord.ini (C:\ACCORD.NT\accord.ini – для 32-битных ОС) для параметра UseLogicalDisksNames изменить значение No (значение по умолчанию) на Yes.
4. Выполнять все дальнейшие действия и настройки ПРД стандартным способом, как описано в документации на СПО «Аккорд».

ВНИМАНИЕ! Если используются логические имена, то невозможно будет разграничить доступ к съемным дискам (флоппи, USB и др.).

2.2. Активация подсистемы разграничения доступа.

Для активации подсистемы разграничения доступа в пункте меню «Команды» выбирайте подпункт «Активация». Подсистема будет установлена и запустится при следующей загрузке.

ВНИМАНИЕ! Программа ACSETUP.EXE предназначена как для установки, так и для снятия подсистемы разграничения доступа, поэтому рекомендуется скопировать эту программу и хранить ее на отдельном магнитном носителе.

ВНИМАНИЕ! Для изменения настроек и дополнительных параметров подсистемы защиты не требуется каждый раз устанавливать/снимать подсистему, достаточно запустить программу ACSETUP.EXE, включить или выключить соответствующие параметры и выйти из программы, сохранив изменения. Исключение составляют параметры «При старте», «Режим сессии» и «Мягкий режим». После изменения этих параметров требуется перезагрузка компьютера.

Для полноценной работы СПО «Аккорд» в каталог, где установлено СПО «Accord-Win64 K», должен быть скопирован файл лицензии Accord.key. Если в каталоге с программным обеспечением этого файла нет, то необходимо запросить файл лицензии (описание процедуры получения файла лицензии см. в п.2.1.3). В этом файле содержится информация о типе продукта (для рабочей станции или терминального сервера). При отсутствии файла или несовпадении контрольной суммы файла процедура инсталляции подсистемы разграничения доступа не выполняется. Если истек срок действия лицензии, то ее можно продлить, прислав файл Accord.key на e-mail key@okbsapr.ru.

2.3. Установка правил разграничения доступа (ПРД) для пользователей

Установка правил разграничения доступа (ПРД) для пользователей СВТ, утвержденных в соответствии с политикой информационной безопасности, принятой в организации (предприятии, фирме и т.д.), осуществляется администратором БИ с использованием программ Aced32.exe или AcedVI.exe. Описание программ, порядок их применения приведены в документах «Установка правил разграничения доступа. Программа ACED32.» (37222406.26.20.40.140.091 97) и «Редактор прав пользователей виртуальной инфраструктуры. Программа AcedVI» (11443195.4012-037 97) из комплекта эксплуатационной документации на СПО «Аккорд-Win64 K». Примеры ПРД приведены в документе «Руководство администратора» (37222406.26.20.40.140.091 90).

2.4. Особенности установки СЗИ Аккорд в системах терминального доступа (СТД)

2.4.1. Установка СЗИ «Аккорд» на терминальном сервере

Программное обеспечение «Аккорд» содержит модули, которые обеспечивают выполнение защитных функций при работе терминального сервера. В качестве серверного ПО может использоваться Windows NT (x86)/ 2000 (x86)/ 2003 (x86)/ 2008 (x86) / 2008 R2/ 2012/ 2012 R2/2016 в стандартной конфигурации или с установленным Citrix Metaframe. Установка программного обеспечения на жесткий диск выполняется стандартным образом. Режим работы (в терминальном режиме или нет) определяется ключом лицензии (Accord.key). При этом различия проявляются только в программе

настройки СПО «Аккорд». В подменю «Параметры» появляется дополнительный пункт «Terminal Server» (рисунок 31).

ВНИМАНИЕ! Для варианта установки СПО «Аккорд» Terminal Server Edition в файле лицензии Accord.key содержится информация о количестве обрабатываемых терминальных сессий. Обратите внимание, что в этом файле параметр [Products] имеет значение Accord TS Edition! Для версий ПО «Аккорд» 4.0.10.51 и выше при несоответствии варианта установки ПО с информацией в файле лицензии выдается сообщение «Ключевой файл лицензии не подходит для этого продукта!», и программа настройки не запускается.

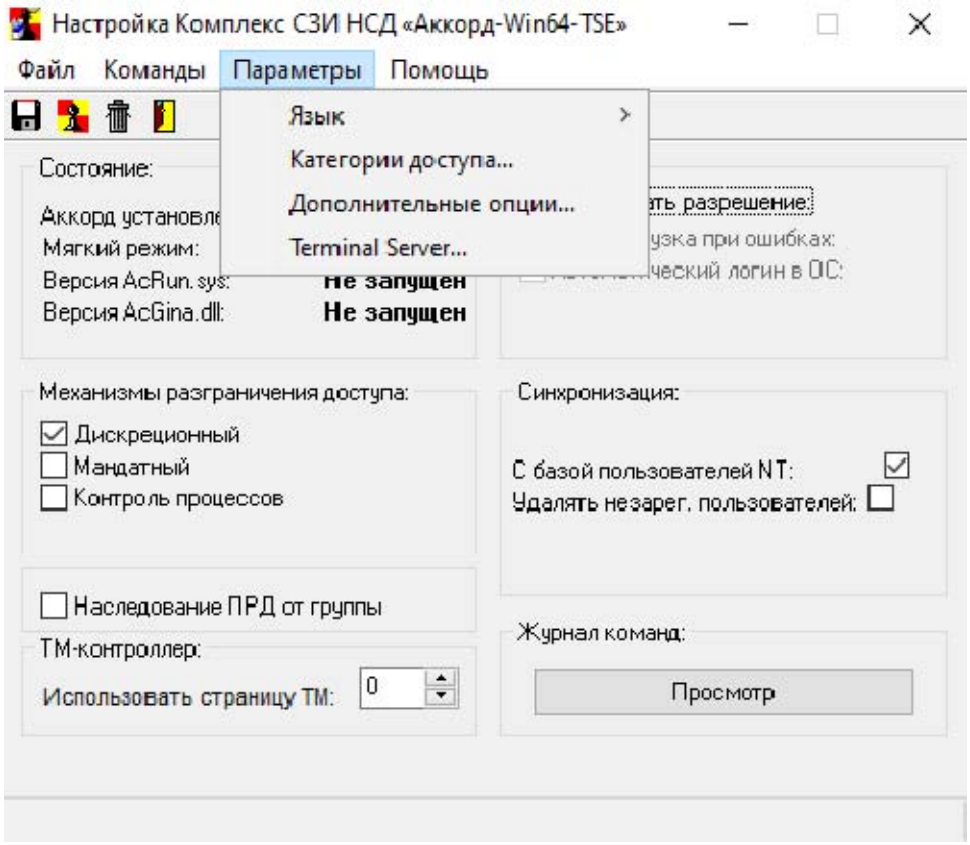


Рисунок 31 - Пункт меню «Terminal Server» в программе настройки СПО «Аккорд»

Выбор пункта «Terminal Server» в меню «Параметры» открывает окно настроек сессий терминального доступа (рисунок 34).

Для начала необходимо выбрать протокол виртуального канала, по которому будет осуществляться связь с терминалами. «Аккорд» поддерживает протокол RDP для Windows Terminal Server и ICA для Citrix Metaframe. Необходимо выбрать хотя бы один протокол, но возможна работа одновременно по двум протоколам.

При выборе протокола ICA в случае, если в системе будет найден продукт Citrix XenDesktop, появится предупреждение, что локальный вход возможен только при нажатии клавиш <ctrl>+<alt>+<delete> (рисунок 32).

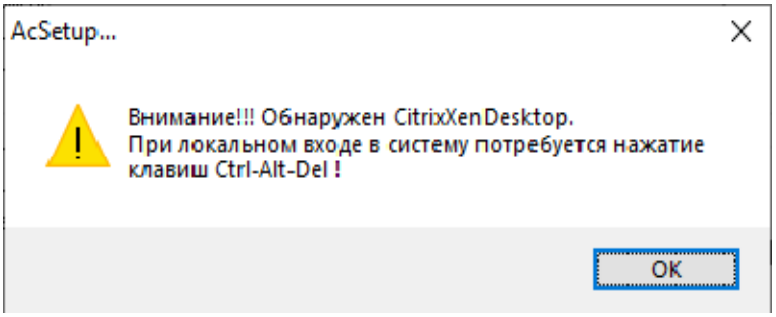


Рисунок 32 - Предупреждение при найденном Citrix XenDesktop

Если при этом в разделе «Дополнительные опции» будет установлен флаг «Использовать проверку подлинности сеанса Windows», а в системе будет находиться продукт Citrix Virtual Delivery Agent без модуля Citrix Receiver, может появиться сообщение о невозможности сквозной идентификации в Citrix XenDesktop (рисунок 33).

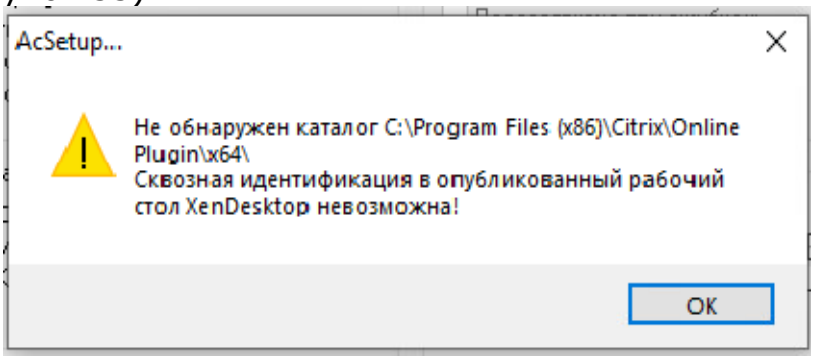


Рисунок 33 - Сообщение о невозможности сквозной идентификации

В случае появления этого сообщения следует переустановить Citrix Virtual Delivery Agent, при этом в процессе установки должен быть выбран компонент Citrix Receiver.

Параметр «Тайм-аут (сек.)» определяет время отклика (в секундах) устройства, подключенного к клиенту. Если по истечении данного времени устройство не успело ответить, запрос клиенту посылается повторно.

ВНИМАНИЕ! В случае если при установленном сервере публикации Citrix Metaframe в процессе запуска утилит из состава ПАК «Аккорд» (версии 5.0.10.59 и выше) возникают ошибки Application Error с кодом 1000, следует в окне настроек сессий терминального доступа (рисунок 34) нажать кнопку <Фильтр Citrix> и перезагрузить сервер.

Будет выполнено изменение необходимых ключей реестра в соответствии с параметрами из файла CitrixHookDisabledProc.txt.

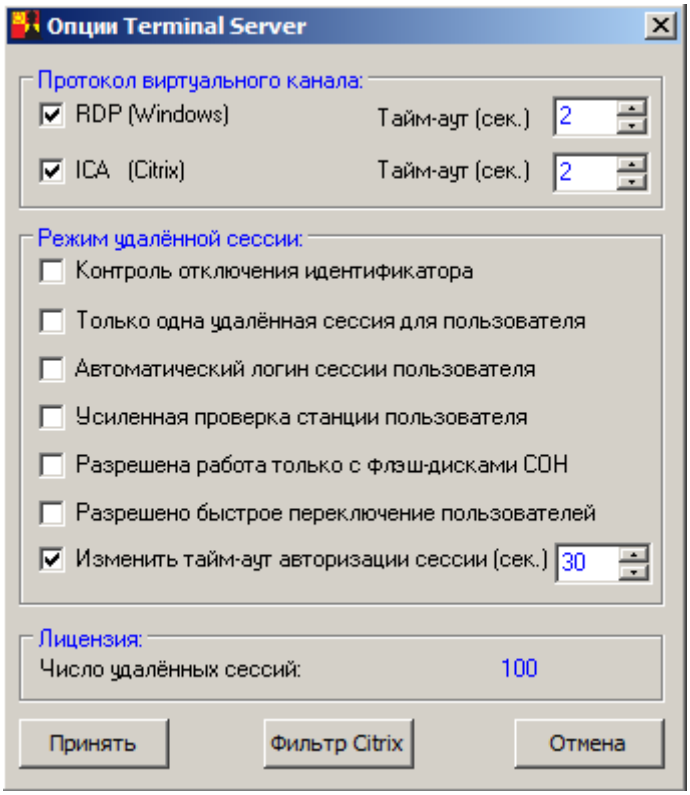


Рисунок 34 - Настройки режимов работы Terminal Server

«Режим удаленной сессии» определяет варианты взаимодействия с клиентскими терминалами.

«Контроль отключения идентификатора»[8] – флаг определяет режим работы сессии пользователя при извлечении идентификатора.

«Только одна удаленная сессия для пользователя» – вариант работы, когда удаленный пользователь не может одновременно открыть несколько удаленных сессий с разных рабочих мест к терминальному серверу. Следует отметить, что в ОС Vista и выше локальные сессии также учитываются: если пользователь включил компьютер, на нем появляется так называемая нулевая сессия от имени этого пользователя (в ней работают системные службы и прочее), а любая попытка войти в систему представляет собой уже вторую сессию. В этом случае ПАК «Аккорд» не предоставит доступ к ОС ни локально, ни удаленно.

«Автоматический логин сессии пользователя» – флаг определяет режим работы пользовательского терминала, при котором результаты идентификации/аутентификации пользователя передаются от клиентской части СПО «Аккорд» программному обеспечению на сервере, которое обрабатывает начало сессии удаленного пользователя.

Если локальные учетные данные пользователя корректны с точки зрения СПО «Аккорд» на терминальном сервере, терминальная сессия пользователя

---

[8] При установке флага «Контроль отключения идентификатора» в программе ACED32.EXE необходимо задать поведение компьютера при извлечении идентификатора из USB-порта компьютера (см. п.7.6. документа «Установка правил разграничения доступа. Программа ACED32» 37222406.26.20.40.140.091 97)

начинается автоматически без запроса дополнительных данных от пользователя. В противном случае ПО «Аккорд» на терминальном сервере выводит сообщение об ошибке и завершает терминальную сессию.

Значение флага «Автоматический логин сессии пользователя» хранится в файле Accord.ini (параметр AutoLoginSession=Yes, если флаг установлен).

«Усиленная проверка станции пользователя» – этот флаг включает режим проверки не только идентификационных параметров пользователя, но также и идентификационных параметров удаленного терминала.

«Разрешена работа только с флеш-дисками СОН»[9] - флаг определяет режим работы с ПАК «Секрет Особого Назначения». Если флаг установлен, то в режиме терминальной сессии разрешена работа только с ПАК «Секрет Особого Назначения», доступ к остальным съемным устройствам запрещен. Если флаг не установлен, то разрешена работа со всеми съемными устройствами, подключенными к рабочей станции.

«Разрешено быстрое переключение пользователей» - флаг определяет режим работы пользовательского терминала, при котором возможно переключение между пользователями терминального сервера с сохранением активных сессий ранее работавших на терминальном сервере пользователей (аналогично функции «Сменить пользователя» в ОС Windows; кнопка «Сменить пользователя» в ОС Windows при установленном флаге «Разрешено быстрое переключение пользователей» не блокируется – как следствие, могут быть открыты несколько одновременных локальных сессий).

«Изменить тайм-аут авторизации сессии (сек.)» – флаг определяет возможность настройки тайм-аута для ожидания авторизации удаленной сессии. Значение флага сохраняется также в файле Accord.ini_save (параметр SessionLogonTimeout).

После выбора нужных опций необходимо выполнить перезагрузку терминального сервера.

Все остальные настройки правил разграничения доступа на сервере не отличаются от стандартных. Администратор создает пользователя, регистрирует его идентификатор, назначает пароль и правила доступа к ресурсам, которые находятся на жестком диске терминального сервера. Особенность администрирования на терминальном сервере заключается в том, что терминальные пользователи должны регистрироваться в отдельной группе, которая будет синхронизироваться не только с группой Users, но и с группой Remote Desktop Users.

В свойствах группы есть параметр «NT группы». Нажав на кнопку в правой части этого поля, мы получим доступ к списку групп в составе ОС и можем выбрать политику синхронизации пользователей СЗИ «Аккорд» с учетными записями в операционной системе (рисунок 35). Как включить пользователя СЗИ «Аккорд» в несколько групп в составе ОС, также описывается в документе «Установка правил разграничения доступа. Программа Aced32.exe» (37222406.26.20.40.140.091 97).

---

9) Флаг «Разрешена работа только с флеш-дисками СОН» доступен только для 64-bit ОС Windows Server 2012 и выше

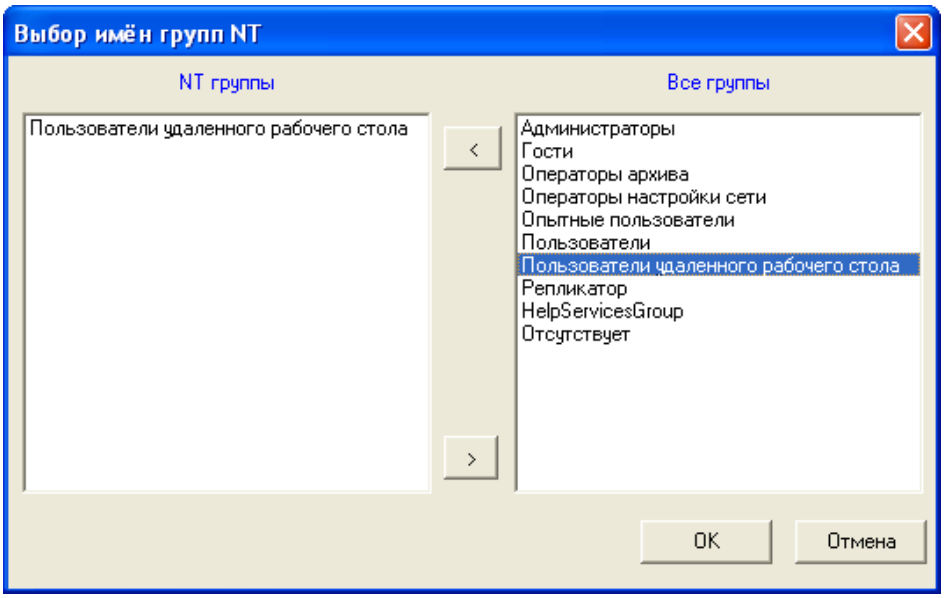


Рисунок 35 - Выбор групп в составе ОС для синхронизации пользователей СЗИ «Аккорд»

2.4.2. Установка клиентского ПО СЗИ «Аккорд» на удаленном терминале

На удаленном терминале устанавливается клиентское ПО СЗИ «Аккорд»:

- из папки Win32_64 дистрибутивного носителя «Аккорд-ТК» для терминалов под управлением ОС Windows используется файл AccordSetupTC.exe;
- из папки Win32_64 дистрибутивного носителя «Аккорд-ТК» для терминалов под управлением ОС Windows, поддерживающих подпись SHA256, используется файл AccordSetupTC_Win7.exe;
- из папки LinTC дистрибутивного носителя «Аккорд-ТК» для терминалов под управлением ОС Linux[10] используются архивы astrace_files, alt_files и astra_files.

После установки ПО необходимо выполнить настройку терминального клиента СЗИ «Аккорд». Последовательно выбирая мышью Пуск> Программы> Аккорд-ТС> Настройка терминального клиента, запустить нужное приложение.

Необходимо выбрать один или оба протокола и тип используемого на терминале персонального идентификатора (рисунок 36).

После выбора параметров следует нажать кнопку <Активировать> для применения настроек службы терминального клиента СЗИ «Аккорд».

[10] В версиях 5.0.10.90 (для 64-битных ОС) и 4.0.10.90 (для 32-битных ОС) появилась возможность установки клиентского ПО на терминалы под управлением ОС семейства Linux. Инструкции по установке СПО СЗИ «Аккорд» для ОС AstraLinux CE Орел, Alt Linux Workstation 9 и AstraLinux SE Смоленск 1.7 приведены в Приложениях 2 – 4.

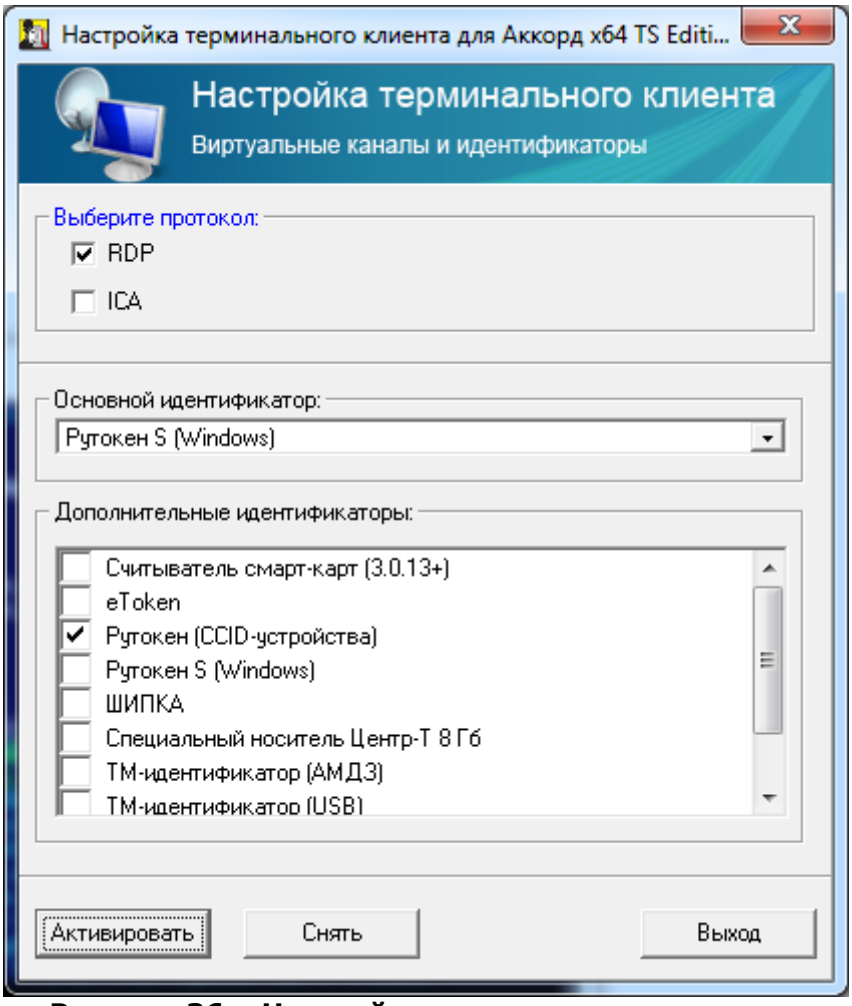


Рисунок 36 – Настройка терминального клиента

После этого привычная процедура подключения к терминальному серверу слегка видоизменяется. После запуска программы mstsc (Microsoft Terminal Server Client) можно обычным образом выбрать сервер или его IP-адрес (рисунок 37).

Рисунок 37 - Выбор терминального сервера

Но после выбора кнопки <Connect> (Подключение) выполняется дополнительная процедура идентификации (рисунок 38). Значение таймера на предъявление идентификатора при подключении к терминальному серверу фиксировано и составляет 20 секунд (по истечении этого времени окно терминального клиента закрывается).

ВНИМАНИЕ! При выполнении процедуры подключения к терминальному серверу с использованием протокола ICA следует в СЗИ «Аккорд» указывать имя пользователя, пароль и имя домена, используемые при логине в ферму Citrix.

ВНИМАНИЕ! В случае если при отключении сессии пользователя и повторном подключении к терминальному серверу, на котором установлен Citrix XenApp/XenDesktop, на экран не выводится окно авторизации пользователя, следует активировать процедуру перевода такой сессии в блокировку посредством установки значения 1 для параметра LockIcaAfterReconnect (REG_DWORD) в следующих ветках системного реестра:

x32 HKEY_LOCAL_MACHINE\SOFTWARE\OKB SAPR\Accord

x64 HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\OKB SAPR\Accord

Если для данного параметра установлено значение 1, то после разрыва ICA сессии и повторного подключения к станции сессия будет переведена в заблокированное состояние. По умолчанию для данного параметра установлено значение 0 (т.е. автоматический перевод сессии в заблокированное состояние при указанных условиях отключен).

ВНИМАНИЕ! При использовании вместо клиента *mstsc.exe* консоли Windows *mmc.exe* с оснасткой «Удаленные рабочие столы» проброс идентификатора в RDP-сессию не поддерживается!

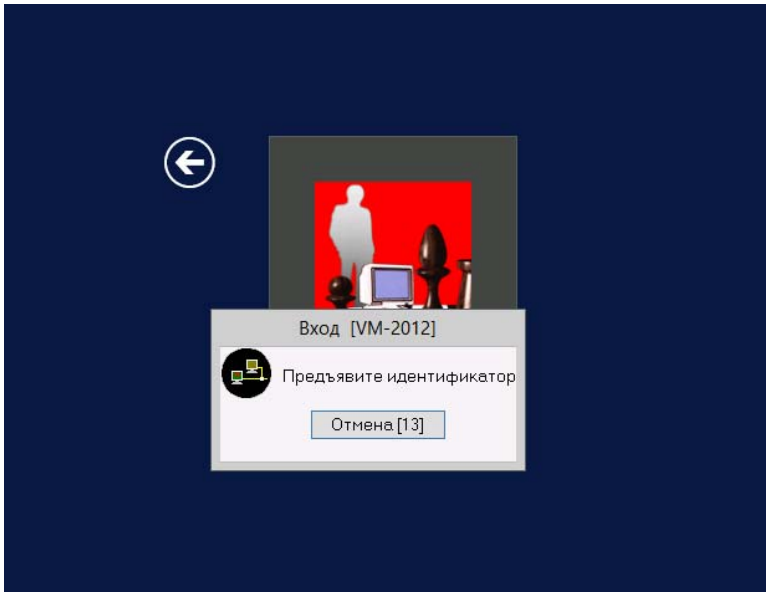


Рисунок 38 - Идентификация пользователя

После предъявления идентификатора необходимо выполнить процедуру аутентификации пользователя (рисунок 39).

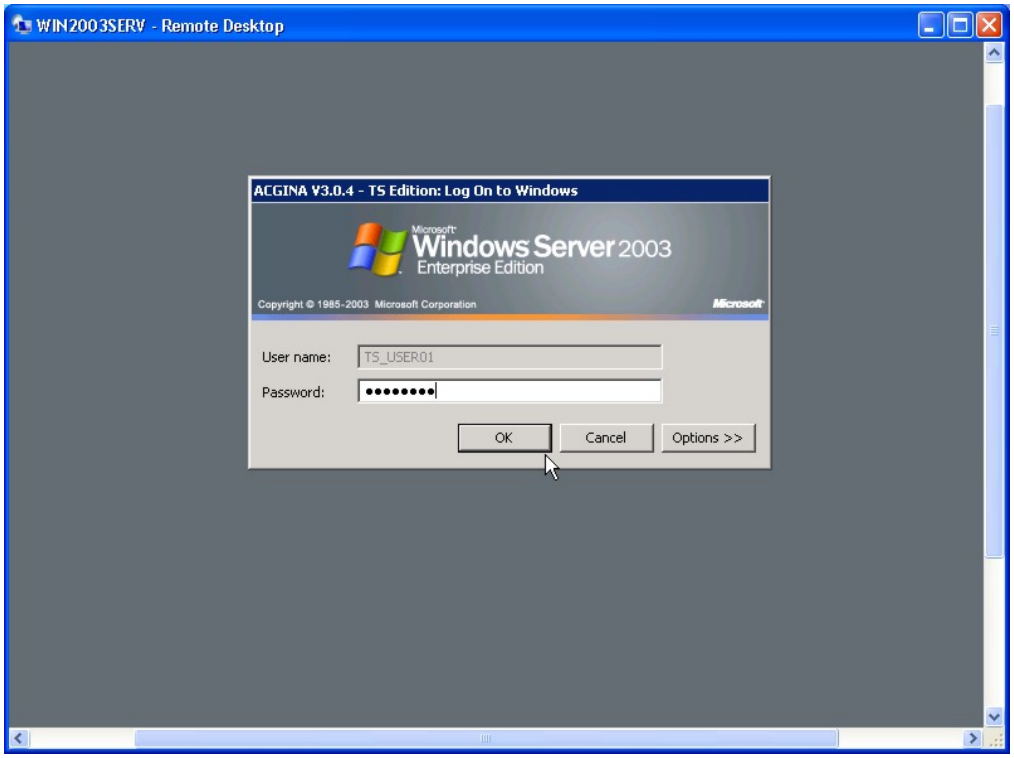


Рисунок 39 - Аутентификация пользователя по паролю

В случае использования устройства ШИПКА идентификатором служит уникальный серийный номер конкретного устройства, который записывается при изготовлении и впоследствии не меняется даже при форматировании внутренней памяти устройства ШИПКА.

Результаты И/А передаются на сервер в защищенном виде, и уже серверная часть СЗИ «Аккорд» ищет учетную запись в своей базе данных. Если пользователь успешно провел процедуру идентификации/аутентификации, то для него открывается сессия с тем набором правил разграничения доступа (ПРД), который установил администратор безопасности на терминальном сервере.

При подключении к нескольким опубликованным приложениям в рамках сессии пользователя процедуру ИА необходимо выполнять только при подключении к первому приложению (Citrix создает одну сессию для всех опубликованных приложений). Следует учитывать, что в рамках одного сеанса недопустимо одновременное использование сессий RDP и Citrix.

На терминальном сервере монитор безопасности СЗИ «Аккорд» функционирует в многопользовательском и многозадачном режиме, т.е. для каждого сеанса терминального пользователя выполняется индивидуальная политика работы с ресурсами сервера, основанная на сертифицированных механизмах дискреционного и мандатного доступа. Реализованная в СЗИ «Аккорд» процедура динамического контроля целостности существенно усиливает стойкость защиты, т.к. исполняемый модуль, включенный в список

контроля, проверяется непосредственно перед каждым запуском, что гарантирует неизменность среды во время всего сеанса работы.

Приведенные на рисунках примеры относятся к тому случаю, когда средой для работы терминального клиента являются ОС Windows 2000/XP/Embedded. Однако специалистами ОКБ САПР разработаны варианты клиентской части и для Windows CE v.5-6, и для Linux (версия ядра 2.6).

ВНИМАНИЕ! Перед выполнением процесса удаления клиентского ПО СЗИ «Аккорд» с удаленного терминала необходимо нажать кнопку <Снять> в окне программы настройки терминального клиента СЗИ «Аккорд» (см. рисунок 36).

Установка и настройка «Аккорд-ТК» возможна также посредством команд, выполняемых в командной строке, со следующими ключами (порядок и регистр ключей не важен):

/install – установить;

/remove – удалить (снять) ключи;

/rdp –поддержка работы с использованием протокола RDP;

/ica - поддержка работы с использованием протокола ICA;

/tm - поддержка работы с ТМ-идентификаторами;

/Tm-Usb - поддержка работы с идентификаторами ТМ-USB;

/shipka - поддержка работы с идентификаторами ШИПКА;

/Cards_New - поддержка работы со считывателями смарт-карт;

/ruToken - поддержка работы с идентификаторами ruToken lite;

/ruToken-S - поддержка работы с идентификаторами ruToken-S;

/eToken - поддержка работы со «старыми» идентификаторами eToken;

/Token#11 - поддержка работы с «новыми» идентификаторами eToken.

Пример:

Для установки «Аккорд-ТК» и активации его с протоколами RDP/ICA и основным идентификатором ruToken lite можно воспользоваться командами со следующими ключами:

AccordSetupTC.exe /quiet

После установки (установка занимает несколько минут) из каталога с Аккорд-ТК (Accord.TC) выполнить команду:

AcSetupTCx64.exe /install /rdp /ica /rutoken /shipka (для 64-битных ОС)

AcSetupTC.exe /install /rdp /ica /rutoken /shipka (для 32-битных ОС)

В этом случае первый ключ идентификатора (/rutoken) будет считаться основным (ruToken lite), а второй (/shipka) – дополнительным (ШИПКА).

Для снятия следует выполнить команду со следующим ключом:

AcSetupTC.exe /remove (для 32-битных ОС)

AcSetupTCx64.exe /remove (для 64-битных ОС)

По ключу /remove удаляются все ключи.

По ключу /install всегда сначала автоматически выполняется ключ /remove.

2.4.3. Описание работы с программой AcTmReg.exe

Встречаются случаи, когда нет возможности использовать при регистрации на терминальном сервере физические идентификаторы пользователей. Например, когда устройства TouchMemory и устройства ШИПКА уже переданы пользователям, и пользователи находятся территориально удаленно от терминального сервера.

В этом случае при регистрации идентификаторов пользователей с помощью программ Aced32 или AcedVI можно выбрать в окне «Операции с ключом пользователя» пункт «Из файла». Далее будет предложено выбрать файл, хранящий описание идентификаторов. Поддерживается два формата файлов: *.amz - стандартная база пользователей Аккорд, и *.atf - файл описания идентификаторов.

Для формирования файла TmId.atf служит программа AcTmReg.exe (рисунок 40).

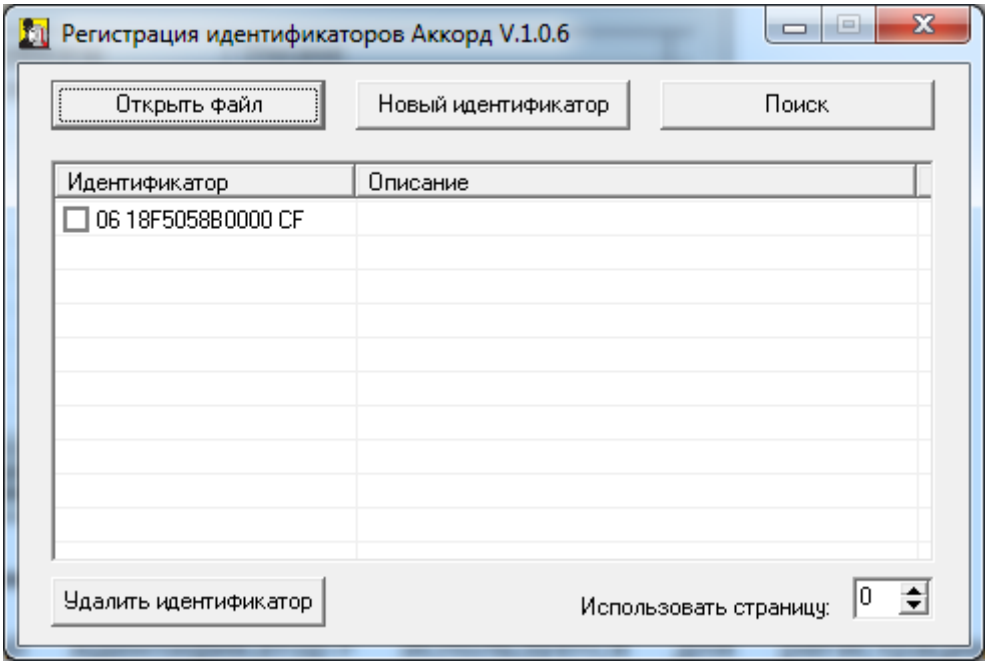


Рисунок 40 – Главное окно программы AcTmReg.exe

Кнопка <Новый идентификатор> используется для регистрации идентификаторов пользователей. По нажатии данной кнопки проверяется, есть ли в идентификаторе ключ пользователя. Если его нет, то будет сформирован новый ключ; если он есть, то на экране появляется окно (рисунок 41):

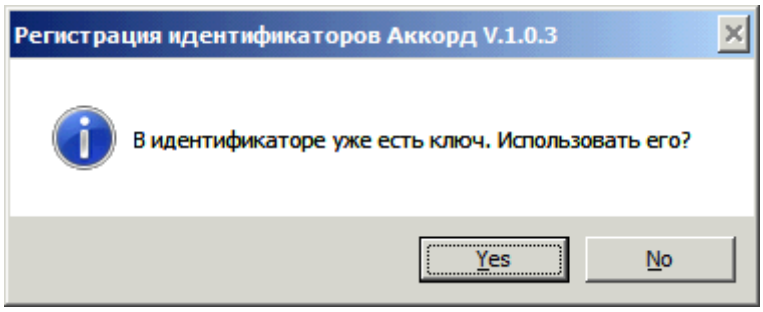


Рисунок 41 – Регистрация идентификатора

Необходимо нажать кнопку <Да>, если планируется использовать старый ключ, и кнопку <Нет>, если нужно создать новый ключ пользователя (рисунок 41).

Далее на экране появляется окно, в котором можно ввести описание идентификатора и нажать кнопку <ОК> (рисунок 42).

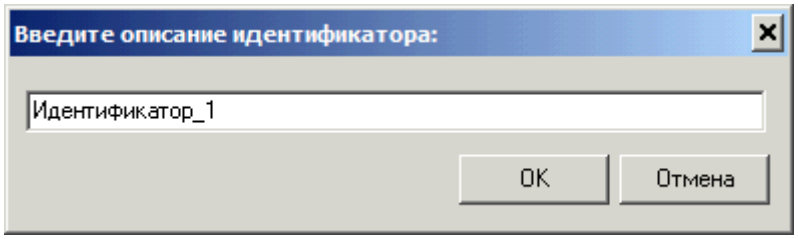


Рисунок 42 – Описание идентификатора

По умолчанию, программа работает с файлом TmId.atf; если нужно работать с другим файлом, то необходимо использовать кнопку <Открыть файл>, при нажатии на которую на экране появляется окно выбора файла (рисунок 43), в котором нужно выбрать соответствующий файл *.atf и нажать кнопку <Открыть>. Допускается выбор сразу нескольких файлов *.atf. В этом случае в каталог старта утилиты AcTmReg.exe будет записан файл с именем Multi.atf. Этот файл можно редактировать, открыв его и дважды щелкнув по полю «Описание». Для быстрого поиска идентификатора следует подключить его и нажать кнопку <Поиск> - идентификатор будет выделен цветом.

ВНИМАНИЕ! При создании .atf файла с группой пользователей для последующего импорта в ПАК «Аккорд» необходимо убедиться, что полные имена пользователей не содержат запрещенных спецсимволов, поскольку при импорте группы пользователей имена пользователей в базе «Аккорд» будут созданы автоматически путем обрезания полного имени пользователя до установленной длины (12 символов) либо до символа "@".

Если в доменном имени пользователя будут использованы запрещенные символы, имя пользователя в «Аккорд» будет установлено как "ATF_#", где #-порядковый номер пользователя с некорректным именем. Также, если идентификатор пользователя уже присутствует в системе, пользователь будет пропущен. Все возникающие ошибки будут описаны в автоматически создаваемом файле "ImportError.log".

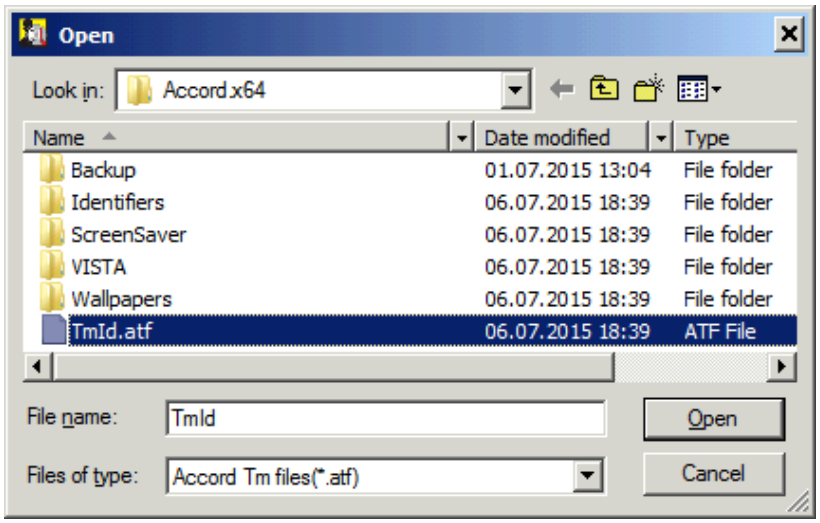


Рисунок 43 - Окно выбора файла *.atf

Параметр «Использовать страницу» по умолчанию установлен в 0. Изменять этот параметр НЕ РЕКОМЕНДУЕТСЯ! В эту и следующую страницу памяти идентификатора записывается ключ пользователя при его регистрации. Изменение этого параметра приведет к тому, что ранее зарегистрированные идентификаторы будут восприниматься системой защиты как недопустимые. Изменение этого параметра возможно, если используется ПО сторонних производителей, которое записывает свою информацию в те же страницы памяти. После изменения этого параметра ВСЕ используемые идентификаторы должны быть перерегистрированы с генерацией нового ключа пользователя.

Регистрация идентификатора возможна также посредством команд, выполняемых в командной строке, со следующими ключами (порядок и регистр ключей не важен):

/file:filename
/desc:Description

Переход на работу с командной строкой осуществляется, если есть хотя бы один ключ.

/file:filename (без указания пути) создает файл в текущем каталоге
/file:filename (с указанием пути) создает файл по указанному пути

Если filename не имеет расширения, то добавляется расширение .atf Если поле filename не заполнено, то программа AcTmReg.exe будет работать с файлом TmId.atf в текущем каталоге.

/desc:Description указывает имя пользователя

Если поле Description не заполнено, то в файле не будет описания для идентификатора.

Максимальное количество символов, используемое в поле Description, не должно быть более 34 – при большем количестве поле будет ограничено 34 символами.

Пример: AcTmReg.exe /file:c:\111.atf /desc: user1@domain.ru

При запуске программы с ключами командной строки вся информация выводится на консоль.

В результате регистрации идентификатора создается файл, содержащий хэш-функцию от ключа пользователя, номера идентификатора и служебных данных. Далее этот файл необходимо переслать администратору безопасности информации терминального сервера любым способом (например, по электронной почте).

2.5. Особенности использования USB-устройств в качестве персональных идентификаторов

При использовании ПАК СЗИ «Аккорд» для защиты терминальных систем может возникнуть ситуация, когда удаленный терминал по своим конструктивным особенностям не предполагает установку каких-либо плат расширения. В этом случае в качестве персонального идентификатора используется USB-устройство.

Для использования в этом качестве устройства ШИПКА необходимо предварительно его инициализировать, прежде чем регистрировать как идентификатор.

Примечание. Все действия по инициализации устройства выполняются однократно для нового устройства и не требуют повторения.

Процедура инициализации выполняется в соответствии с документацией в составе СПО ACShipka Environment. При первом подключении ШИПКА в USB-порт необходимо установить драйвер для этого устройства.

Если в качестве персонального идентификатора планируется использовать Специальный носитель Центр-Т 8Гб, на терминале должно быть установлено соответствующее ПО. Необходимая информация об этом содержится в документации на Специальный носитель Центр-Т 8Гб.

Для использования ruToken-S потребуется предварительная инициализация токена в соответствии с инструкцией «Инициализация токенов ruToken-S для работы с комплексом «Аккорд-АМДЗ».

2.6. Особенности работы с сетевыми дисками в СПО «Аккорд»

Работа с сетевыми дисками в СПО «Аккорд» имеет некоторые особенности.

Для корректной работы СПО «Аккорд» рекомендуется монтировать сетевые ресурсы под той же учетной записью, под которой выполняется вход в операционную систему. Данная логика предусматривает отсутствие возможности выполнения несанкционированных действий под другими учетными записями в рамках текущей сессии.

В случае необходимости монтирования сетевого ресурса под учетной записью, отличной от той, под которой был выполнен вход в ОС, необходимо вводить учетные данные сетевого пароля во вторую строку запроса учетной записи (кроме доступа к Web-ресурсу) (рисунок 44).

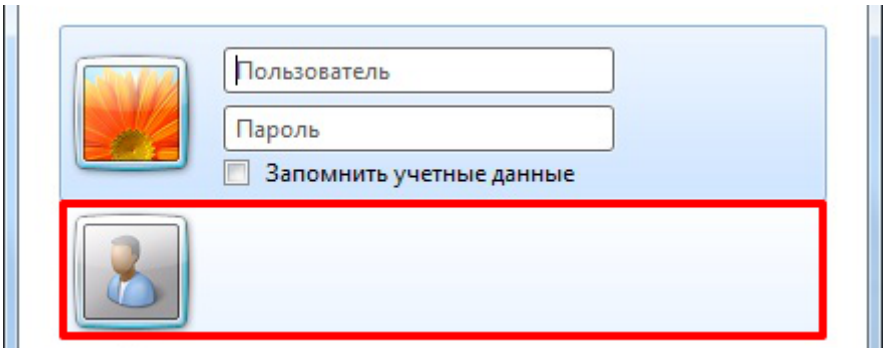


Рисунок 44 - Ввод сетевого пароля при подключении сетевого диска

ВНИМАНИЕ! При подключении к сетевому диску из того же домена логин учетной записи следует вводить без указания домена.

При подключении к сетевому диску из другого домена логин учетной записи следует вводить с указанием домена.

3. Смена режима работы СПО «Аккорд»

Начиная с версии 5.0.10.51 ПО «Аккорд» выпускается с единым дистрибутивом для локальной и терминальной версий – AccordSetup-K.exe/ AccordSetupWin64-K.exe. Процесс установки локальной и терминальной версий выглядит одинаково, различается только содержимое ключевого файла лицензии.

При необходимости смены режима работы уже установленного СПО «Аккорд» (локальный на терминальный и наоборот) следует деактивировать СПО «Аккорд» (см. раздел 4) и выполнить активацию с соответствующим ключом лицензии (см. п.2.2).

4. Снятие средств защиты СПО «Аккорд-Win64 K»

ВНИМАНИЕ! Снятие защиты разрешено только администратору БИ (супервизору)[11].

Перед выполнением процедуры снятия защиты СПО «Аккорд» необходимо на ПК в локальных политиках безопасности в параметры «Архивация файлов и каталогов», «Восстановление файлов и каталогов» добавить группу «Администраторы». Иначе при попытке выполнить процедуру снятия на экране появится сообщение: «Не хватает привилегий Windows для модификации реестра».

Для снятия защиты необходимо выполнить следующие действия:

1. Включить и войти в систему с параметрами администратора БИ.
2. Запустить программу ACSETUP.EXE из каталога \ACCORD.X64 (\ACCORD.NT – для 32-битных ОС). При этом повторно запрашивается идентификатор администратора БИ. Если идентификация администратора БИ прошла успешно, то на экран выводится главное окно программы настройки СПО «Аккорд».
3. В пункте меню «Команды» следует выбрать подпункт «Снятие». Система разграничения доступа будет отключена и при следующей загрузке не будет активироваться. Каталог ACCORD.X64 (\ACCORD.NT – для 32-битных ОС) остается на жестком диске. Для полной деинсталляции системы «Аккорд» необходимо перезагрузить компьютер и запустить процедуру удаления ПО Аккорд в панели управления компьютера.

[11] При этом администратор должен обладать привилегиями "Редактирование настроек", "Редактирование пользователей", "Редактирование журналов" и "Редактирование контроля", устанавливаемыми в редакторе параметров доступа Aced32 или AcedVI

5. Удаление СПО «Аккорд-Win64 К»

ВНИМАНИЕ! Перед выполнением процедуры удаления СПО «Аккорд-Win64 К» необходимо выполнить снятие средств защиты СПО «Аккорд».

Чтобы удалить СПО «Аккорд-Win64 К», необходимо выбрать Панель управления\Установка и удаление программ\Комплекс СЗИ НСД «Аккорд-Win64 К» и нажать кнопку <Удалить>.

Если перед выполнением процедуры удаления СПО «Аккорд» не выполнено снятие средств защиты, то при попытке удаления СПО «Аккорд» на экране появится сообщение:

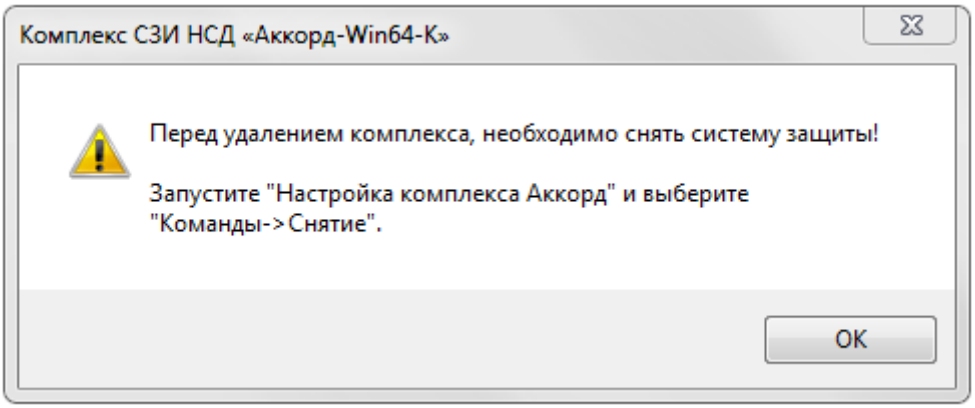


Рисунок 45 – Сообщение при попытке удаления СПО «Аккорд-Win64 К» без выполнения снятия средств защиты «Аккорд»

Приложение 1.
Формат журнала AcEvents.log

В журнал AcEvents.log заносятся сведения о каждом входе пользователя в ОС Windows. В общем случае вход в ОС записывается строкой следующего формата:

Тип входа	Дата ДД.ММ.ГГГГ	Время ЧЧ.ММ.СС	Имя компьютера	Имя пользователя	Login или Unlck	Результат входа	Идентификатор пользователя	Серийный номер идентификатора

Поле «Тип входа» содержит значения «ACRUN:» или «Logon:».

ACRUN: - авторизация на этапе старта ОС, когда от Аккорд-АМДЗ в монитор разграничения доступа Acrun.sys передаются значения параметров Результаты И/А, в большинстве случаев используется для запуска нулевой сессии.

Logon: - вход в Windows через модуль AcGina.dll. При включении ПК могут использоваться данные от АМДЗ (результаты И/А), при открытии нового сеанса запрашивается идентификатор пользователя.

ВНИМАНИЕ! Для 64-разрядных ОС, начиная с Windows 7, при включении ПК в журнал заносятся две записи:

ACRUN:15.04.2019 09:05:41 ADMINIB SUPERVISOR Login OK [0C 0216227B0000 18,SN = 35005051]
Logon: 15.04.2019 09:05:41 ADMINIB SUPERVISOR(Администратор@ADMINIB) Login OK [0C 0216227B 0000 18, SN=35005051]

В поле «Имя компьютера» записывается собственное имя компьютера.

Поле «Имя пользователя» заполняется в следующем формате:
Имя пользователя Аккорда(Имя пользователя Windows@Имя домена Windows)

Значение «Unlck» в следующем поле означает разблокировку сессии.

При наличии в записи события имени пользователя в два последних поля заносятся идентификатор и его серийный номер в следующем формате:

[идентификатор пользователя, SN = серийный номер идентификатора]

Поле «Результат входа» может содержать следующие значения:

OK – успешный вход в ОС;

Error, unknown user – неизвестный пользователь;

Incorrect password or username – некорректный пароль или имя пользователя;

UNKNOWN Login Acrun.sys: TM-driver not found! Invite Administrator!!! – неизвестный логин, не найден ТМ-драйвер, пригласите администратора;

UNKNOWN Login Ошибка проверки объектов! Пригласите АИБа!!!;

Учетная запись пользователя заблокирована из-за долгого бездействия! Пригласите АИБа!!!

Лицензия истекает через … дней! WARNING;

Истек срок действия лицензии! ERROR;

Wrong Secret Key – неправильный секретный ключ;

UNKNOWN Login Identifier is not registered! – неизвестный логин, идентификатор не зарегистрирован;

UNKNOWN Login Error geting user Identifier from TBM!. Timeout! [ErrCode = 000000FE] – неизвестный логин, ошибка передачи Результатов И/А, выход по таймауту;

Error = 1 – фатальная ошибка ACRUN.

Приложение 2. Установка СПО СЗИ «Аккорд» на терминал под управлением ОС AstraLinux CE Орел

Установка СПО СЗИ «Аккорд» на терминал под управлением ОС AstraLinux CE Орел проводится в несколько этапов в соответствии с нижеприведенной последовательностью действий.

Этап 1. Подготовительные работы

1.1. Открыть терминал и повысить привилегии до root.

1.2. Скопировать на компьютер директорию astrace_files (находится на дистрибутивном носителе «Аккорд-ТК»), содержащую необходимые библиотеки Аккорд-ТК. В текущей инструкции директория скопирована в /home/user/.

1.3. Перейти в каталог командой *cd /home/user/astrace_files/*

1.4. Установить службу смарт-карт и сопутствующие пакеты командой apt-*get install pcscd libpcsclite1 pcsc-tools libccid opensc opensc-pkcs11*

Этап 2. Установка модуля работы с идентификатором Рутокен ЭЦП

2.1. Установить пакет ifd-rutokens с официального сайта Рутокен.

Этап 3. Установка модуля работы с идентификатором Шипка Лайт

3.1. Вариант 1. Добавить в файл /etc/libccid_Info.plist следующие строки:

<key>ifdVendorID</key>
<array>
.....
<string>0x17E4</string>
</array>
....
<key>ifdProductID</key>
<array>
.....
<string>0x0040</string>
</array>
<key>ifdFriendlyName</key>
<array>
.....
<string>SHIPKA LITE Slim</string>
</array>

Вариант 2. Скопировать настроенный файл из архива командой *cp libccid_Info.plist /etc/libccid_Info.plist*

3.2. Перезапустить сервис PCSC командой *systemctl restart pcscd*

Этап 4. Установка модуля работы USB-TM идентификатора

4.1. Скопировать скомпилированный модуль TM-идентификатора в каталог с модулями ядра командой

cp tmusb_drv.ko /lib/modules/4.15.3-3-generic/kernel/

4.2. Скопировать необходимое для работы правило UDEV из архива в соответствующий каталог командой *cp 99-tmusb.rules /etc/udev/rules.d/*

4.3. Пересоздать список зависимостей модулей командой *depmod*

4.4. Перезагрузить правила UDEV командой

udevadm control -R && udevadm trigger

Этап 5. Установка библиотек поддержки идентификаторов для работы с виртуальными каналами

5.1. Скопировать из архива библиотеки командой *cp -a libtmid/* /usr/lib/*

5.2. Переформировать кэш библиотек при помощи команды *ldcofnig*

Этап 6. Установка библиотеки для работы виртуальных каналов в клиенте Citrix Workspace App

6.1. Скопировать из архива библиотеку работы с виртуальными каналами в папку с установленным клиентом командой *cp tm-ica.so /opt/Citrix/ICAClient/*

6.2. Вариант 1. Внести изменения в файл настроек клиента Citrix /opt/Citrix/ICAClient/config/module.ini:

- в раздел [ICA 3.0] в строке VirtualDriver через запятую добавить модуль виртуального канала CTmDrv32;

- перед разделом [Compress] добавить следующие строки:

[CTmDrv32]

DriverName=tm-ica.so

Вариант 2. Скопировать преднастроенный файл настроек командой

cp module.ini /opt/Citrix/ICAClient/config/

Приложение 3. Установка СПО СЗИ «Аккорд» на терминал под управлением ОС Alt Linux Workstation 9

Установка СПО СЗИ «Аккорд» на терминал под управлением ОС Alt Linux Workstation 9 проводится в несколько этапов в соответствии с нижеприведенной последовательностью действий.

Этап 1. Подготовительные работы

1.1. Открыть терминал и повысить привилегии до root.

1.2. Скопировать на компьютер директорию alt_files, содержащую необходимые библиотеки Аккорд-ТК. В текущей инструкции директория скопирована в /home/user/.

1.3. Перейти в каталог командой *cd /home/user/alt_files/*

1.4. Удалить конфликтующие пакеты командой

apt-get remove -y pcsc-lite-openct libopenct openct

1.5. Обновить базу репозитория Альт Линукс командой *apt-get update*

1.6. Установить службу смарт-карт и сопутствующие пакеты командой

apt-get install pcsc-lite opensc pcsc-tools pcsc-lite-ccid

Этап 2. Установка модуля работы с идентификатором Рутокен ЭЦП

2.1. установить пакеты поддержки модуля Rutoken командой

apt-get install librtpkcs11ecp pcsc-lite-rutokens

Этап 3. Установка модуля работы с идентификатором Шипка Лайт

3.1. Вариант 1. Добавить в файл /usr/lib64/pcsc/drivers/ifd-ccid.bundle/Contents/Info.plist следующие строки:

<key>ifdVendorID</key>
<array>
.....
<string>0x17E4</string>
</array>
....
<key>ifdProductID</key>
<array>
.....
<string>0x0040</string>
</array>
<key>ifdFriendlyName</key>
<array>
.....

<string>SHIPKA LITE Slim</string>

</array>

Вариант 2. Скопировать настроенный файл из архива командой

cp Info.plist /usr/lib64/pcsc/drivers/ifd-ccid.bundle/Contents/Info.plist

Этап 4. Установка модуля работы USB-TM идентификатора

4.1. Скопировать скомпилированный модуль TM-идентификатора в каталог с модулями ядра командой

cp tmusb_drv.ko /lib/modules/5.4.51-std-def-alt1/kernel

4.2. Скопировать необходимое для работы правило UDEV из архива в соответствующий каталог командой *cp 99-tmusb.rules /etc/udev/rules.d/*

4.3. Пересоздать список зависимостей модулей командой *depmod*

4.4. Перезагрузить правила UDEV командой

udevadm control -R && udevadm trigger

Этап 5. Установка библиотек поддержки идентификаторов для работы с виртуальными каналами

5.1. Скопировать из архива библиотеки командой

cp -a libtmid/ /usr/lib64/*

5.2. Переформировать кэш библиотек при помощи команды *ldcofnig*

Этап 6. Установка библиотеки для работы виртуальных каналов в клиенте Citrix Workspace App

6.1. Скопировать из архива библиотеку работы с виртуальными каналами в папку с установленным клиентом командой *cp tm-ica.so /opt/Citrix/ICAClient/*

6.2. Вариант 1. Внести изменения в файл настроек клиента Citrix /opt/Citrix/ICAClient/config/module.ini:

- в раздел [ICA 3.0] в строке VirtualDriver через запятую добавить модуль виртуального канала CTmDrv32;

- перед разделом [Compress] добавить следующие строки:

[CTmDrv32]

DriverName=tm-ica.so

Вариант 2. Скопировать преднастроенный файл командой

cp module.ini /opt/Citrix/ICAClient/config/

Приложение 4. Установка СПО СЗИ «Аккорд» на терминал под управлением ОС AstraLinux SE Смоленск 1.7

Установка СПО СЗИ «Аккорд» на терминал под управлением ОС AstraLinux SE Смоленск 1.7 проводится в несколько этапов в соответствии с нижеприведенной последовательностью действий.

Этап 1. Подготовительные работы

1.1. Открыть терминал и повысить привилегии до root.

1.2. Скопировать на компьютер директорию astra_files, содержащую необходимые библиотеки Аккорд-ТК. В текущей инструкции директория скопирована в /home/user/.

1.3. Перейти в каталог командой *cd /home/user/astra_files/*

1.4. Установить службу смарт-карт и сопутствующие пакеты: libusb-0.1.4, pcscd, libpcsclite1, pcsc-tools, libccid, opensc, opensc-pkcs11

Этап 2. Установка модуля работы с идентификатором Рутокен

2.1. Установить пакет ifd-rutokens с официального сайта Рутокен.

Этап 3. Установка модуля работы с Шипка Лайт

3.1. Вариант 1. Добавить в файл /usr/lib64/pcsc/drivers/ifd-ccid.bundle/Contents/Info.plist следующие строки:

<key>ifdVendorID</key>
<array>
.....
<string>0x17E4</string>
</array>
....
<key>ifdProductID</key>
<array>
.....
<string>0x0040</string>
</array>
<key>ifdFriendlyName</key>
<array>
.....
<string>SHIPKA LITE Slim</string>
</array>

Вариант 2. Скопировать настроенный файл из архива командой
cp Info.plist /usr/lib64/pcsc/drivers/ifd-ccid.bundle/Contents/Info.plist

Этап 4. Установка библиотек поддержки идентификаторов для работы с виртуальными каналами

4.1. Скопировать библиотеки командой *cp -a libtmid/* /usr/lib/*

4.2. Переформировать кэш библиотек при помощи команды *ldcofnig*

Этап 5. Установка библиотеки для работы виртуальных каналов в клиенте Citrix Workspace App

5.1. Скопировать из архива библиотеку работы с виртуальными каналами в папку с установленным клиентом командой *cp tm-ica.so /opt/Citrix/ICAClient/*

5.2. Вариант 1. Внести изменения в файл настроек клиента Citrix /opt/Citrix/ICAClient/config/module.ini:

- в раздел [ICA 3.0] в строке VirtualDriver через запятую добавить модуль виртуального канала CTmDrv32;

- перед разделом [Compress] добавить следующие строки:

[CTmDrv32]

DriverName=tm-ica.so

Вариант 2. Скопировать преднастроенный файл командой

cp module.ini /opt/Citrix/ICAClient/config/

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

№	Содержание изменения (обновления)	Дата	Примечание
1			
2			
3			
4			
5			
6			