Secret Disk Enterprise 2.7.5

Руководство по обновлению ОС MS Windows

Версия	Версия 2.0
Статус	Публичный
Дата	09.04.2019
Номер	ID-номер

Оглавление

1. Введение

Настоящий документ содержит руководство администратора безопасности сервера SDMS, используемого в продуктах SDE версии 2.7.5 и SD5NET версии 2.7.5, при установке обновлений MS Windows уровня ядра, требующих временного снятия защиты с системного диска рабочей станции с установленным агентом SDA.

Описываются рекомендации по подготовке жесткого диска рабочей станции к безопасной эксплуатации и процессы, сопровождающие обновления ОС.

2. Технология установки обновлений Windows уровня ядра

В настоящем разделе разбираются основные типы обновлений ОС Windows.

2.1 Условная классификация обновлений

Все обновления Microsoft можно условно разделить на три класса:

- обновления приложений Microsoft (Office, Visio, Project etc.):
  - в большинстве случаев не требует перезагрузки, а менеджер обновлений предлагает закрыть и заново открыть используемое приложение;
  - в редких случаях предлагает перезагрузить систему.
- обновление компонентов ОС:
  - в большинстве случаев требует перезагрузки системы для того, чтобы после перезагрузки был подгружен обновленный драйвер или компонент;
  - в редких случаях компонент может быть перезагружен в память "на лету", если данный вид сервиса сейчас не используется.
- обновление ядра (сборки):
  - наиболее сложный в реализации вариант обновления, предполагающий замену главных механизмов ОС;
  - производится только через загрузчика ОС, заменяющий файлы ядра на новые.

> *Именно третий вариант обновлений вступает в конфликт с программным обеспечением Secret Disk, если системный диск защищен (зашифрован).*
>
> *Также с весны 2018 года появилось обновление, направленное на борьбу с вирусами. Такие обновления называют SSU (Service Stack Update). Такое обновление может выходить чаще, чем обновление сборки, но также вызывать конфликт с зашифрованным диском.*

2.2 Типы конфликтов с ПО Secret Disk

Условно все типы конфликтов можно разделить на 2 класса:

1. Изменение размера диска.
2. Замена загрузчика.
3. Замена стека драйверов.

> *Первые два изменения блокируются программным обеспечением Secret Disk 5 NET или Secret Disk Enterprise, если изменение касается зашифрованных дисков.*

Отсутствие блокировки после замены загрузчика приведет к критической системной ошибке (BSoD).

> *Требуется перезапуск компьютера и запуск ОС в режиме safe mod (безопасный режим) и деинсталляция продуктов Secret Disk.*

2.2.1 Изменение размера диска

Это первая и необязательная часть (она касается только дисков с некорректной разбивкой).

> *О рекомендованной разбивке жесткого диска подробно написано в следующем разделе.*

Ошибка происходит из-за того, что драйвер ОС "не видит", что весь раздел зашифрован. ОС, не замечая границ зашифрованного диска, пытается изменить размер. В Secret Disk драйвер шифрования тома работает по номеру сектора, вычисляя ключ шифрования и преобразуя сектора из определенного диапазона. Если отключить блокировку изменения размера тома, то освободившееся, с точки зрения ОС, место будет по-прежнему шифроваться. Но доступно на чтение это пространство будет только в ОС, при запущенном Secret Disk.

Поэтому специальная функция в драйвере блокирует изменение размера зашифрованного тома.

Когда ОС требуется это? В следующих случаях:

- пользователь обновляет ОС с Windows 7 на Windows 10 при зашифрованном системном томе: В Windows 7 не было раздела MSR;
- пользователь имеет разбивку диска с минимальным размером раздела восстановления: новый туда не помещается;
- пользователь на Windows 8 включил "автоматическую установку всех типов обновлений", диск не имеет свободного неразмеченного пространства и др.

> *Чтобы упростить эксплуатацию и минимизировать потери безопасности при обновлении рекомендуется придерживаться рекомендованной схемы разбивки разделов.*

2.2.2 Замена загрузчика UEFI (второй этап обновления ядра)

Наиболее ярко обновление проявляется на ОС MS Windows 10. Начиная с этой версии, компания-производитель перестала создавать внешние версии, изменяя ОС изнутри.

Вне зависимости от того, была попытка изменения системного диска или логического тома, или нет, при замене ядра ОС обязательно произойдет замена загрузчика, о чем ОС внесёт запись в файл, определяющий порядок загрузки.

При перезагрузке с обновлением ядра система не будет загружать обычный стек драйверов, а будет заниматься обновлением (заменой) файлов ядра, чтобы после очередной перезагрузки стартовало новое ядро. Специальные функции драйвера системного тома блокируют изменения, сообщая об этом серверу управления (для версий SDE и SD5 NET).

Для корректного обновления ядра сервер управления SDMS, получая специальные извещения от рабочих станций, может подготовить рабочие станции к установке обновлений.

2.2.3 Обновление стека обслуживания (стека драйверов)

При установке обновлений типа SSU операционная система производит множественную перезагрузку, однако, она отличается от привычных нам "холодной" и "горячей" перезагрузок: она неполная, не обращается к загрузчику, используя свой, промежуточный. На защищённом диске С такой вариант ускоренной перезагрузки проходит до определённого момента: пока системе не требуется перегрузить весь стек драйверов. В этом случае обновленная система может пропустить загрузку драйвера системного диска Secret Disk. Поскольку всё пространство диска зашифровано, то система просто "теряет" диск С. Это равносильно его удалению из системы, после чего делает "откат" памяти в прежнее состояние, чтобы не повредить данные.

Наше программное обеспечение не вмешивается в процесс установки обновлений – это наша принципиальная позиция, и связана она прежде всего с безопасностью информации наших пользователей. Кроме того, редко, но случается, что обновления операционной системы приводят к ошибкам в работе компьютера. А это значит, что может потребоваться восстановление некоторых файлов. Но на защищенном и не смонтированном системном диске операционная система, загруженная, к примеру, с CD-диска, не сможет произвести операцию восстановления.

Именно поэтому, мы считаем необходимым снятие защиты с системного диска на время установки сложных обновлений.

3. Рекомендации по подготовке жесткого диска для установки ОС Windows

В большинстве случаев системные администраторы используют разметку жесткого диска, производимую ОС при установке, или устанавливают новую ОС поверх ранее установленной, сохраняя устаревшую разметку.

В настоящем разделе приведены требования к разметке жесткого диска при планировании использования ПО линейки Secret Disk. Требования основаны на официальных рекомендациях MSDN.MICROSOFT.COM.

3.1 Общая информация

> *В настоящем документе не рассмотрен узкий сегмент рынка ПК, использующий устаревшую версию EFI (класс 1), которая использует структуру разделов GUID (GPT).*

3.1.1 Встроенное ПО

UEFI (класс 2): использует структуру разделов GPT. Также содержит модуль поддержки совместимости (CSM), который позволяет использовать функции BIOS, включая структуру разделов MBR. Этот модуль во встроенном ПО можно включить или отключить. При планировании использования Secret Disk настоятельно рекомендуем отключить модуль и использовать полноценную структуру GPT.

UEFI (класс 3): использует структуру разделов GPT.

BIOS: использует структуру разделов MBR (master boot record – основная загрузочная запись).

3.1.2 Системный раздел

Устройство должно содержать системный раздел. На дисках GPT он называется системным разделом EFI или ESP. Раздел обычно хранится на основном жестком диске. Устройство загружается в этот раздел.

Минимальный размер раздела составляет 100 МБ, а для дисков Advanced Format – 260 МБ, и он должен быть отформатирован в формате файлов FAT32.

3.1.3 MSR-раздел

В Windows 10 для дисков на базе UEFI/GPT был уменьшен рекомендованный размер раздела MSR со 128 МБ до 16 МБ, однако рекомендуется сохранить раздел равным 128 МБ для сохранения совместимости. Размеры современных жестких дисков достаточны, чтобы не фокусироваться на экономии 100 МБ.

3.1.4 Раздел Windows

Раздел должен занимать не менее 20 ГБ дискового пространства для 64-разрядных версий и не менее 16 ГБ для 32-разрядных. Раздел Windows необходимо отформатировать в NTFS.

Рекомендуется создавать раздел минимум 40ГБ. Оптимальным значением будет (40ГБ+Размер ОЗУ). Так для наиболее распространенных ПК с ОЗУ 4 ГБ раздел будет иметь размер 44 ГБ.

3.1.5 Раздел средств восстановления

В разделе должно быть достаточно места для образа средств среды восстановления Windows (winre.wim, обычно 250–300 МБ, в зависимости от добавленного базового языка и настроек), а также достаточно свободного пространства, чтобы служебные программы резервного копирования могли записать раздел.

Если раздел от 300МБ до 500 МБ, то необходимо минимум 50 МБ свободного пространства.

Если раздел больше 500 МБ, то необходимо минимум 320 МБ свободного пространства.

Если раздел больше 1 ГБ, рекомендуется минимум 1 ГБ свободного пространства.

Для этого раздела необходимо использовать ИД типа: DE94BBA4-06D1-4D40-A16A-BFD50179D6AC.

> *Рекомендуется делать раздел размером 1 ГБ и оставлять после него 1 ГБ свободного пространства.*
>
> *Это позволит Windows изменять и повторно создавать раздел, если для будущих обновлений потребуется образ для восстановления большего размера.*

3.1.6 Раздел пользовательских данных

Большинство данных пользователя (рабочий стол, документы, изображения, музыка и т.д.) могут быть перенаправлены на логический том (раздел диска, не содержащий программ ОС). Такое расположение упрощает обновление системы и облегчает системным администраторам создание резервных копий пользовательских данных.

Таких разделов может быть несколько, но достаточно одного.

3.2 Подготовка HDD для компьютеров со встроенным ПО UEFI BIOS классы 2, 3

Рисунок 1. Макет разбиения UEFI/GPT диска по умолчанию

В приведённом ниже примере командного файла DISKPART показано как можно корректно подготовить жесткий диск к установке ОС Windows от версии 7 до версии 10.

В примере, чтобы избежать возможных конфликтов, назначаются следующие буквы дискам:

S – System;

W – Windows (после перезагрузки этому разделу автоматически будет присвоена буква C);

U – User Data (после перезагрузки этому разделу автоматически будет присвоена буква D);

R – Recovery.

> *Буква X не может быть использована, поскольку она зарезервирована для среды предустановки Windows.*
>
> *Все данные на первом (по счёту) жёстком диске будут утеряны после его разбиения.*

Приведённый ниже пример необходимо сохранить в текстовый файл UEFI-GPT.txt и сохранить на внешнем USB-накопителе.

```
rem == UEFI-GPT.txt ==
rem == Данные команды предназначены для программы DiskPart
rem    для создания пяти разделов на UEFI-GPT компьютере.
rem == При необходимости установите нужные размеры
rem    разделов, соответствующие Вашим требованиям ==
select disk 0
rem == Следующая команда полностью очистит диск!
rem == Если требуется сохранить раздел с заводским образом,
rem == скорректируйте файл!
clean all
convert gpt
rem == 1. System partition ========================
```

```
create partition efi size=260
format quick fs=fat32 label="System"
assign letter="S"
rem == 2. Microsoft Reserved (MSR) partition ======
create partition msr size=128
rem == 3. Windows partition ========================
create partition primary size=44000
format quick fs=ntfs label="Windows"
assign letter="W"
rem == 4. User Data partition ======================
create partition primary
shrink minimum=2000
format quick fs=ntfs label="User Data"
assign letter="U"
rem == 5. Recovery tools partition ================
create partition primary
shrink minimum=1000
format quick fs=ntfs label="Recovery tools"
assign letter="R"
set id="de94bba4-06d1-4d40-a16a-bfd50179d6ac"
gpt attributes=0x8000000000000001
list volume
exit
```

Предположим, что внешний USB-накопитель имеет букву F, тогда запуск разбиения диска на выполнение должен быть выполнен командой:

```
DiskPart /s F:\UEFI-GPT.txt
```

3.3 Подготовка HDD для компьютеров со встроенным ПО BIOS (Legacy BIOS)

При развертывании Windows на устройстве на основе BIOS жёсткие диски необходимо форматировать с помощью файловой системы MBR.

> *Windows не поддерживает файловую систему GPT (таблица с GUID разделов) на компьютерах на основе BIOS.*

У диска MBR может быть до четырех стандартных разделов. Обычно эти стандартные разделы назначаются основными разделами.

При использовании рекомендованного разбиения на разделы этого количества достаточно, однако, диск может содержать раздел от производителя (обычно в конце разметки), который потребуется сохранить.

Рисунок 2. Макет разбиения BIOS/MBR диска по умолчанию

Буквы разделов назначаются аналогично примеру для GPT выше.

Раздел восстановления для BIOS/MBR компьютера должен иметь идентификатор 27.

Приведённый ниже пример необходимо сохранить в текстовый файл BIOS-MBR.txt и сохранить на внешнем USB-накопителе.

```
rem == BIOS-MBR.txt ==
rem == Данные команды предназначены для программы DiskPart
rem    для создания четырех разделов на BIOS-MBR компьютере.
rem == При необходимости установите нужные размеры
rem    разделов, соответствующие Вашим требованиям ==
select disk 0
```

```
clean
rem == 1. System partition ======================
create partition primary size=100
format quick fs=ntfs label="System"
assign letter="S"
active
rem == 2. Windows partition ======================
create partition primary size=44000
format quick fs=ntfs label="Windows"
assign letter="W"
rem == 3. User Data partition ====================
rem == В данном примере для данных пользователя создаётся
rem == основной раздел. При существовании раздела производителя
rem == необходимо использовать команды создания расширенных
rem == разделов.
create partition primary
shrink minimum=2000
format quick fs=ntfs label="User"
assign letter="U"
rem == 4. Recovery tools partition ==============
create partition primary
shrink minimum=1000
format quick fs=ntfs label="Recovery"
assign letter="R"
set id=27
list volume
exit
```

Предположим, что внешний USB-накопитель имеет букву F, тогда запуск разбиения диска на выполнение должен быть выполнен командой:

```
DiskPart /s F:\BIOS-MBR.txt
```

3.4 Подготовка HDD для компьютеров со встроенным ПО BIOS (Legacy BIOS), содержащим раздел восстановления производителя.

Зачастую диск, который приходит вместе с ноутбуком, содержит "OEM-recovery" раздел, в котором производитель хранит драйвера и образ OEM-системы. В 99% случаев этот образ не понадобится, но большинство администраторов предпочитает сохранить этот раздел. Предположим, что администратор средствами оснастки внешней ОС, например, WinPE, переместил этот раздел в конец физического диска.

Тогда рекомендуемая структура диска будет выглядеть следующим образом:

Рисунок 3. Макет разбиения BIOS/MBR диска по умолчанию

Приведённый ниже пример необходимо сохранить в текстовый файл BIOS-MBR2.txt и сохранить на внешнем USB-накопителе.

```
rem == BIOS-MBR2.txt ==
rem == Данные команды предназначены для программы DiskPart
rem    для создания четырех разделов на BIOS-MBR компьютере.
rem == При необходимости установите нужные размеры
rem    разделов, соответствующие Вашим требованиям ==
select disk 0
rem == 1. System partition ======================
create partition primary size=100
```

```
format quick fs=ntfs label="System"
assign letter="S"
active
rem == 2. Windows partition =====================
create partition primary size=44000
format quick fs=ntfs label="Windows"
assign letter="C"
rem == 3. Extended partition ====================
create partition extended
rem == 4. User Data partition ===================
create partition logical
shrink minimum=2000
format quick fs=ntfs label="User"
assign letter="U"
rem == 5. Recovery tools partition ==============
create partition logical
shrink minimum=1000
format quick fs=ntfs label="Recovery"
assign letter="R"
set id=27
list volume
exit
```

Пусть внешний USB-накопитель имеет букву F, тогда запуск разбиения диска на выполнение должен быть выполнен командой:

```
DiskPart /s F:\BIOS-MBR2.txt
```

3.5 Перенос данных пользователя в раздел USER DATA

3.5.1 Цель переноса

В настоящее время большинство клиентов высоко ценят непрерывность бизнеса, что означает постоянную высокую доступность пользовательской информации без понижения её защищённости.

В то же время, этому противоречит "конфигурация по умолчанию" или "от OEM-производителя", создающая ОДИН диск для программ и данных, а также ежегодные обновления ядра ОС, требующие снятия защиты с диска С.

Также при "едином" диске С трудно снимать образ ОС и установленных программ для последующего быстрого восстановления, неудобно делать резервные копии документов, поскольку они редко остаются лишь в каталоге Documents, если пользователь имеет право записи на диске С, и, наконец, для установки обновлений ядра требуется полное расшифрование системного диска, а чем диск больше, тем дольше он расшифровывается и зашифровывается обратно.

Таким образом, единая цель переноса – повышение надёжности компьютера в целом, за счет оптимизации размещения данных без снижения уровня защищённости.

3.5.2 Рекомендации по переносу

Шифрование файлов профиля пользователя – задача сложная. Однако, в подавляющем большинстве случаев достаточно перенести на логический том наиболее часто используемые пользователями папки, не участвующие в аутентификации:

- Contacts (Список контактов);
- Desktop (Рабочий стол пользователя);
- Documents (Документы пользователя);
- Downloads (Каталог загрузки файлов из Интернета по умолчанию);

- Favorites (Выбранные страницы в MS IE или MS EDGE);
- Links (Ссылки на переменные среды пользователя для других программ);
- Music (Звуковые файлы пользователя);
- Pictures (Изображения пользователя);
- Videos (Видеозаписи пользователя).

Все эти каталоги находятся в папке C:\USERS*username*\ и не влияют на авторизацию пользователя. Это важно, поскольку при применении Secret Disk и отключении защиты системного диска авторизация пользователя в Secret Disk производится ***после*** авторизации пользователя в ОС.

> *Чтобы быть уверенным, что файлы пользователя останутся в безопасности (даже после снятия защиты жесткого диска), рекомендуем их хранить на зашифрованном логическом томе.*

Создаём на диске D:\ папку с именем пользователя. Это проще сделать приведённым ниже командным файлом. Файл помещается в корневую папку диска D: и запускается с аргументом – именем пользователя.

> *Поскольку права на папки наследуются от корневой, рекомендуется разрешить на весь том полный доступ только группе Администраторы, запретив пользователям даже чтение.*

Из приведенного ниже примера сознательно исключены проверки реестра и команды создания новых символьных ссылок: только создание структуры папок. Это позволит не исправлять ссылки, если при запуске будет ошибка, и не приведёт к доступу в папки других пользователей этого компьютера.

```
@echo off
d:\
cd \
if "%1"=="" goto label_1 else goto label_2
:label_2
set username=%1
md %username%
cd %username%
md Contacts
md Desktop
md Documents
md Downloads
md Favorites
md Links
md Music
md Pictures
md Videos
cd ..
echo Directories for user %username% were created
goto label_3
:label_1
echo This batch file needs username as an argument
echo If username contains spacebars use quotas
:label_3
```

Если структура папок для пользователя была успешно создана и проверена, переходим в папку C:\USERS\username нашего переносимого пользователя.

Наводим указатель "мыши" на переносимую папку, делаем щелчок правой клавишей и выбираем из выпадающего контекстного меню "Свойства" ("Properties").

В свойствах выбираем закладку "Расположение" ("Location"), меняем на новое местоположение и нажимаем ниже на кнопку "MOVE".

Убеждаемся в переносе и выбираем следующую из набора папку.

> *При переносе система переносит и права на эту папку: необходимо после окончания переноса авторизоваться под учетной записью перенесённого пользователя и проверить расположение личных папок.*

3.6 Защита пользовательских данных на диске D:

Пользовательские данные на диске USER DATA должны всегда быть защищены как минимум двумя способами:

1. Диск D должен быть зашифрован прозрачным шифрованием. Поскольку шифрование является вторичным и защищает в основном от кражи и утери ноутбука, то лучше выбрать алгоритм с аппаратным ускорением криптографических вычислений, предоставляемый ОС: AES256.
2. Документы и иные важные для пользователя файлы, такие как сканированные копии контрактов в папке Pictures или звукозаписи выступлений в папке Music, должны храниться как минимум на 1 уровень глубже и в защищенных папках.

То есть, пользователь должен инициировать создание защищенных папок там, где он сохраняет конфиденциальную информацию. Например,

```
D:\
     \sergey.ivanov\
              \Contacts\
              \Desktop\
              \Documents\
                       \My_Work•\
                       \Personal_Data•\
                       \Contracts•\
              \Downloads\
              \Favorites\
              \Links\
              \Music\
              \Pictures\
              \Videos\
```

Папки "My_Work", "Personal_Data" и "Contracts", (наименования произвольные и взяты только для примера), являются зашифрованными, то есть информация в файлах, лежащих в этих папках доступна только легитимному пользователю.

Применяя такую конфигурацию, даже снимая защиту с системного диска, администратор безопасности имеет возможность не допускать утечки конфиденциальной информации пользователя.

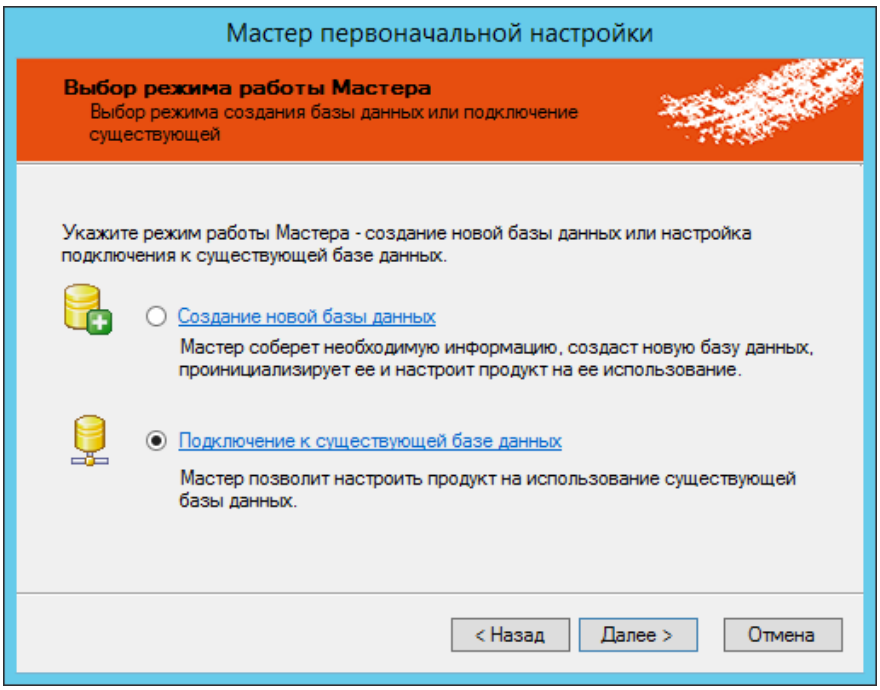
4. Установка обновлений MS Windows

В разделе описывается механизм, реализованный в продукте Secret Disk Enterprise версии 2.7 (SDE 2.7) и в SD5NET версии 2.7. Описываемый функционал не добавляет принципиально новые свойства к настоящим продуктам, но позволяет визуализировать изменения, происходящие на рабочей станции при обновлении ядра ОС.

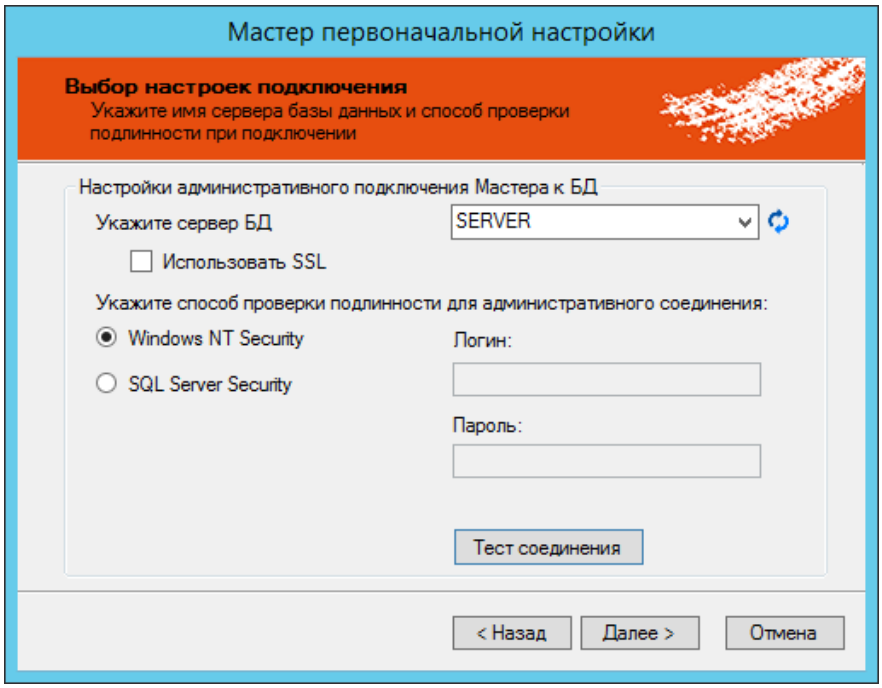
4.1 Переход SDMS на версию 2.7.5

Для обновления версии приложения SDMS на 2.7 с более ранних (2.5.x и старше) выполните следующие действия:

1. Убедитесь, что было успешно проведено резервное копирование базы данных.
2. Откройте **Панель управления компьютера → Удаление программ → Aladdin Secret Disk Management Server → Удалить.**
3. Дождитесь окончания процесса удаления SDMS.
4. Удалите приложение Crypto Extension Pack (CeP).
5. Дождитесь окончания процесса удаления CeP.
6. Перезапустите компьютер.
7. Установите новую версию CeP, выбрав при инсталляции те же криптоалгоритмы и/или криптопровайдеры, установленные ранее.
8. Перезапустите компьютер.
9. Установите новую версию приложения SDMS согласно руководству администратора.
10. Выполните подключение к существующей Базе данных:



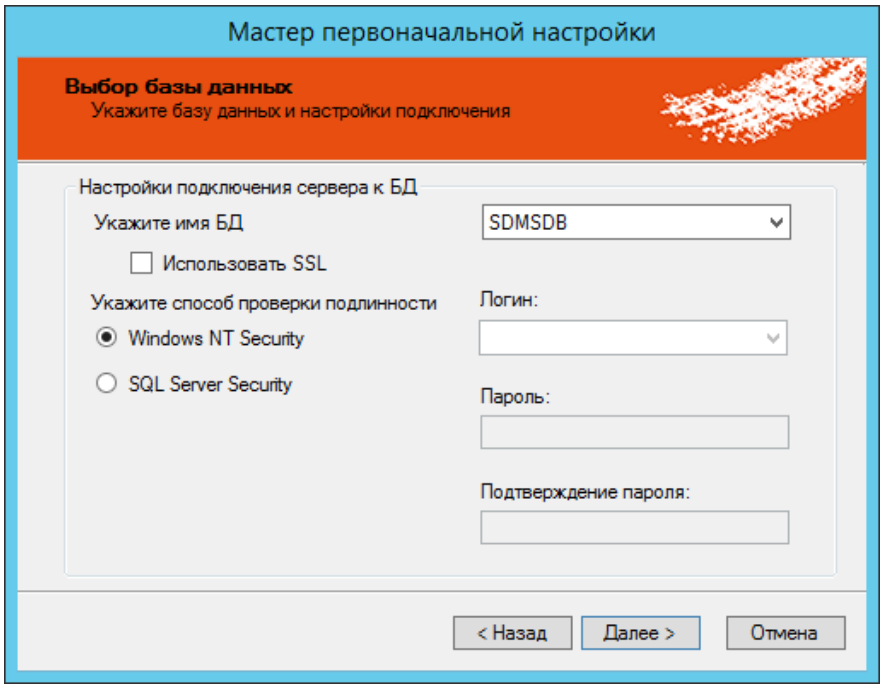
1. Укажите сервер БД, под управлением которого находится существующая БД.



В списке серверов могут отображаться не все имеющиеся экземпляры Microsoft SQL Server, т.к. определение серверов БД в сети не является гарантированным. Если нужный экземпляр SQL Server не отображается в списке, следует ввести его полное имя вручную.

2. Если вы хотите использовать соединение по протоколу SSL, отметьте пункт *Использовать SSL*.
3. Укажите способ проверки подлинности для административного соединения:
   - *Windows NT Security*: используется текущая доменная учётная запись;
   - *SQL Server Security*: для авторизации в полях *Логин* и *Пароль* необходимо указать имя и пароль учётной записи пользователя Microsoft SQL Server.
4. Для проверки соединения с сервером БД нажмите кнопку *Тест соединения*. При успешном соединении появится окно с сообщением *Соединение с сервером успешно установлено*.
5. Нажмите *Далее*.
6. Введите имя базы данных в поле *Укажите имя БД* и выберите способ логина:
   - *Windows NT Security*: используется учётная запись пользователя Windows;
   - *SQL Server Security*: здесь можно указать существующую учётную запись (поле *Логин*) или создать новую, отметив пункт *Создать новый логин* и указав новый пароль в полях *Пароль* и *Подтверждение пароля* (пароль должен иметь длину не менее 8 символов и включать символы следующих типов: цифры, спецсимволы и буквы в верхнем и нижнем регистре).

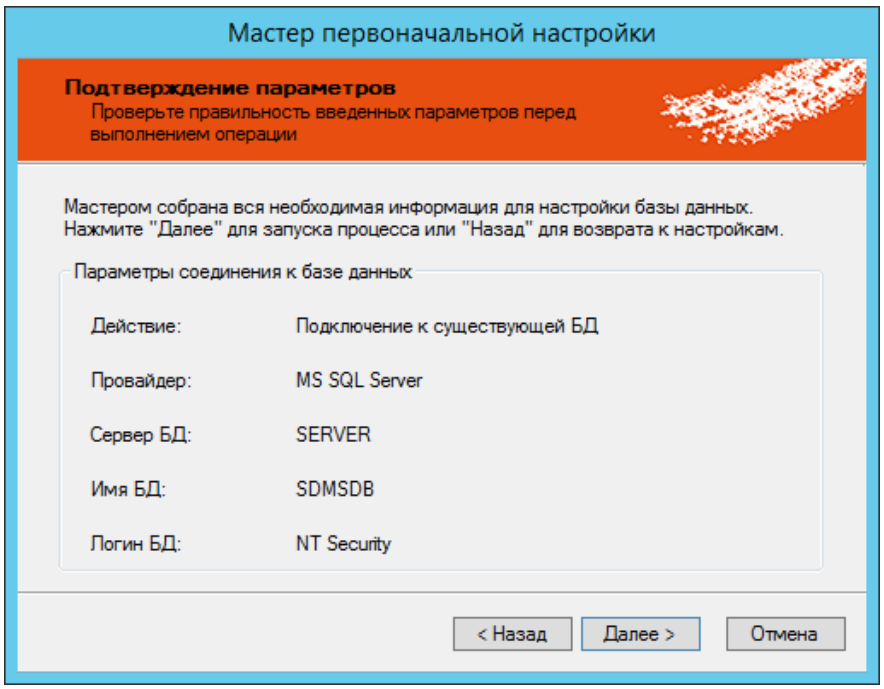
7. Нажмите *Далее*.



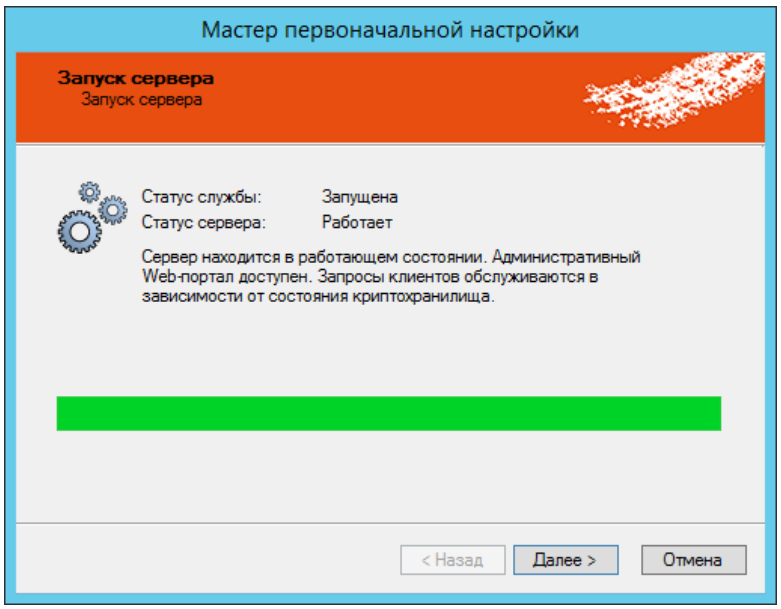
8. Если на этапе подключения к существующей базе данных будет обнаружено, что её версия ниже минимально поддерживаемой сервером, то будет предложено выполнить обновление БД. Дождитесь завершения операции обновления базы данных. Этот процесс может занять несколько минут — в зависимости от объёма данных.

Перед началом обновления базы данных настоятельно рекомендуется выполнить резервное копирование существующей версии базы данных. Кроме того, по возможности, следует завершить все ранее начатые операции с дисками.

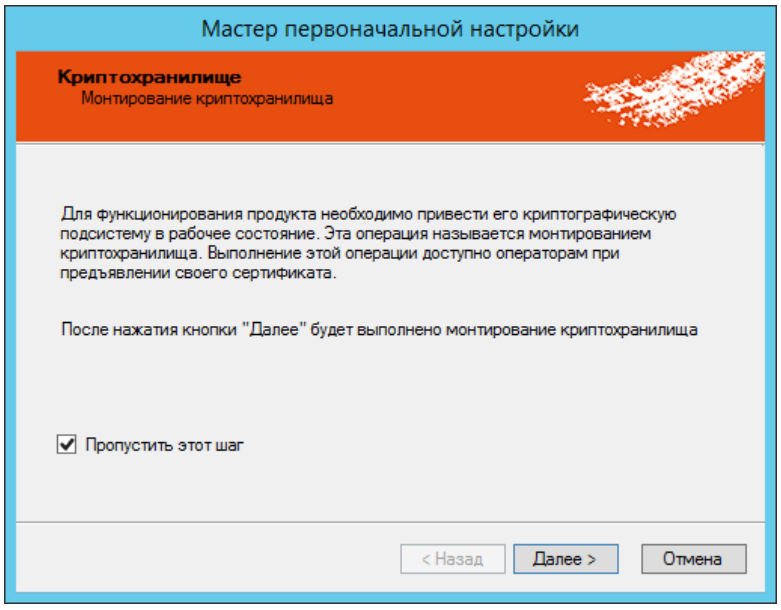
9. После завершения обновления мастер укажет актуальную версию базы данных. Нажмите *Далее*.



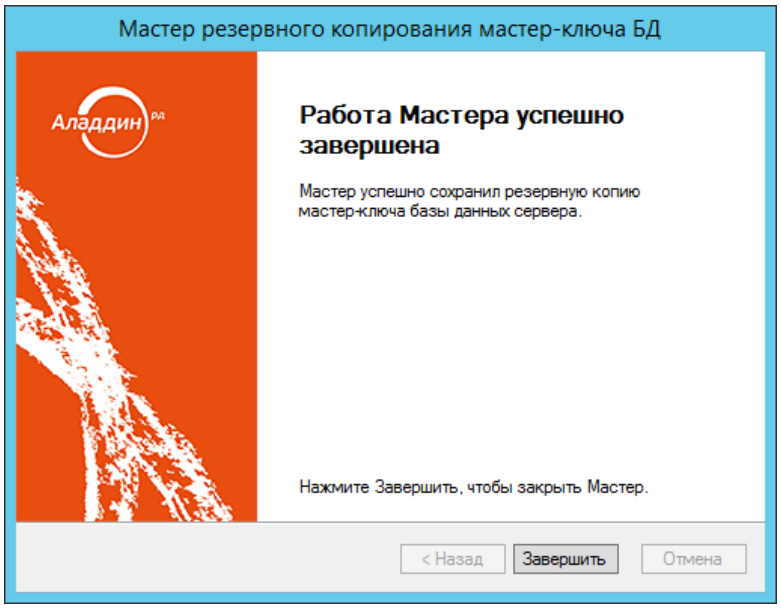
10. После подключения к базе данных мастер переходит к запуску сервера SDMS. Нажмите Далее.



11. Для немедленного монтирования криптохранилища уберите флаг *Пропустить этот шаг* и нажмите Далее.
    Для подключения криптохранилища позже поставьте флаг *Пропустить этот шаг* и нажмите Далее.



12. Нажмите Завершить.



4.2 Режим обновления

Под режимом обновления мы понимаем следующее:

- временное снятие защиты с системного диска на рабочей станции с установленным компонентом SDA (Secret Disk Agent) при срабатывании защиты от модификации диска или загрузчика обновлением либо для установки накопительных обновлений ОС.

Перевод в режим позволяет:

- отслеживать (фильтровать) рабочие станции, на которых произошло срабатывание защиты;
- группировать станции, находящиеся в режиме обновления, включая следующие состояния:
  - станция защищена, но сработала защита;
  - станция в режиме обновления: процесс расшифрования;
  - станция в режиме обновления: Системный диск расшифрован (станция готова к установке обновлений);
  - станция в режиме обновления: процесс зашифрования (возврат из режима обновления).

Таким образом, перевод рабочей станции в режим обновления эквивалентен снятию защиты (расшифрованию) системного диска с последующей установкой защиты. Однако, для контроля состояния рабочих станций, для которых важны одновременно и актуальность применяемой версии ОС, и зашифрованное состояние системного диска с обязательной двухфакторной аутентификацией, применяемый в настоящей версии режим обновления упрощает работу администраторам безопасности, визуализируя состояние защищённости.

4.3 Состояния рабочей станции с установленным SDA

В базовой версии ПО (SDMS 2.5-2.7) для отображения рабочей станции (дисков рабочей станции), присутствовало три состояния:

- защита на диск установлена (диск зашифрован);
- защита на диск не установлена (диск не зашифрован);
- ключ шифрования зашифрованного диска скомпрометирован (диск требует перешифрования).

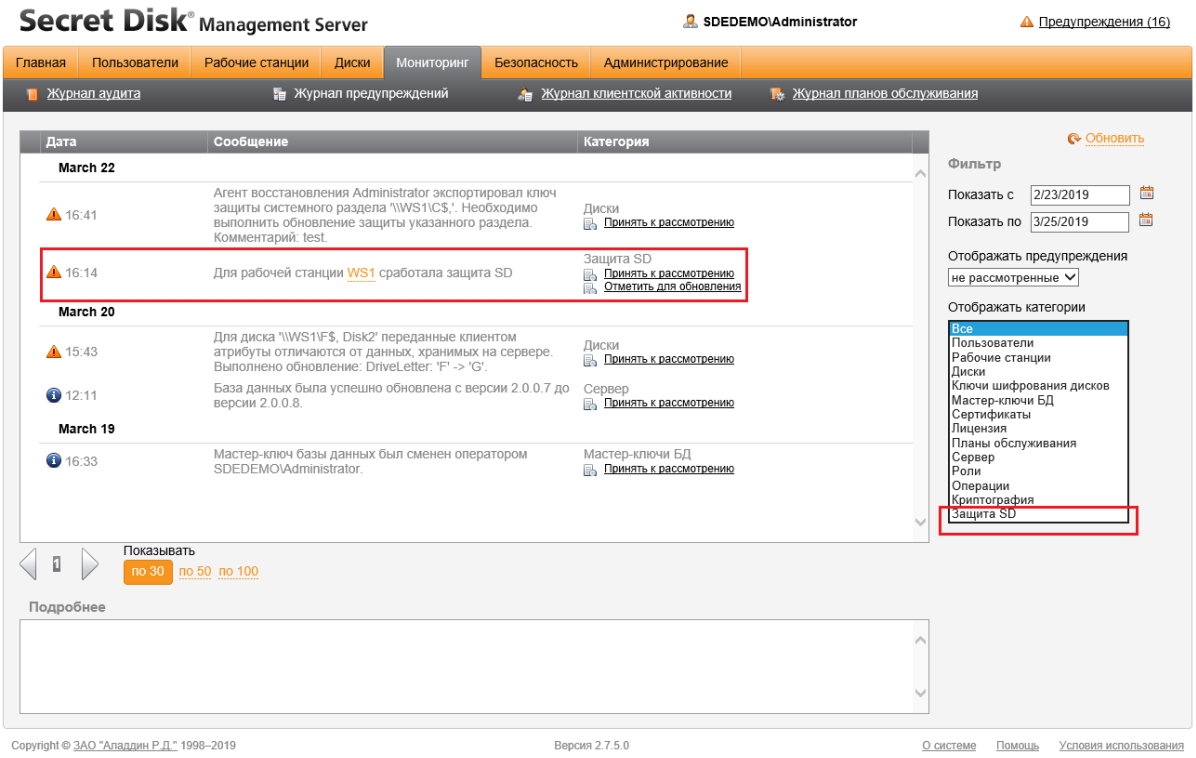
В настоящей версии ПО добавлены четыре состояния режима обновления, перечисленные в предыдущем параграфе.

4.4 Сигнализация о срабатывании защиты на рабочей станции

Уведомление о срабатывании защиты отображается в **Журнале предупреждения** меню **Мониторинга**.

Для отображения срабатывания защиты выделена отдельная категория – **Защита SD**.

В окне фильтра появился новый параметр для фильтрации.



Ссылка с названием станции – активная. При нажатии на неё портал открывает вкладку *Рабочие станции* и помечает выбранную станцию флагом.

4.5 Порядок перевода рабочей станции в режим обновления

В таблице 1 представлены обозначения (метки) рабочих станций, необходимые для обновления ОС.

Таблица 1 – Описание состояний рабочих станций

Значок	Описание
	Рабочая станция отмечена для начала режима обновления.
	Подготовка к обновлению. Начался процесс расшифрования системного диска.
	Рабочая станция готова к обновления ОС. *Системный раздел рабочей станции не защищён!*
	Возврат в рабочее состояние. Начался процесс зашифрования системного диска.

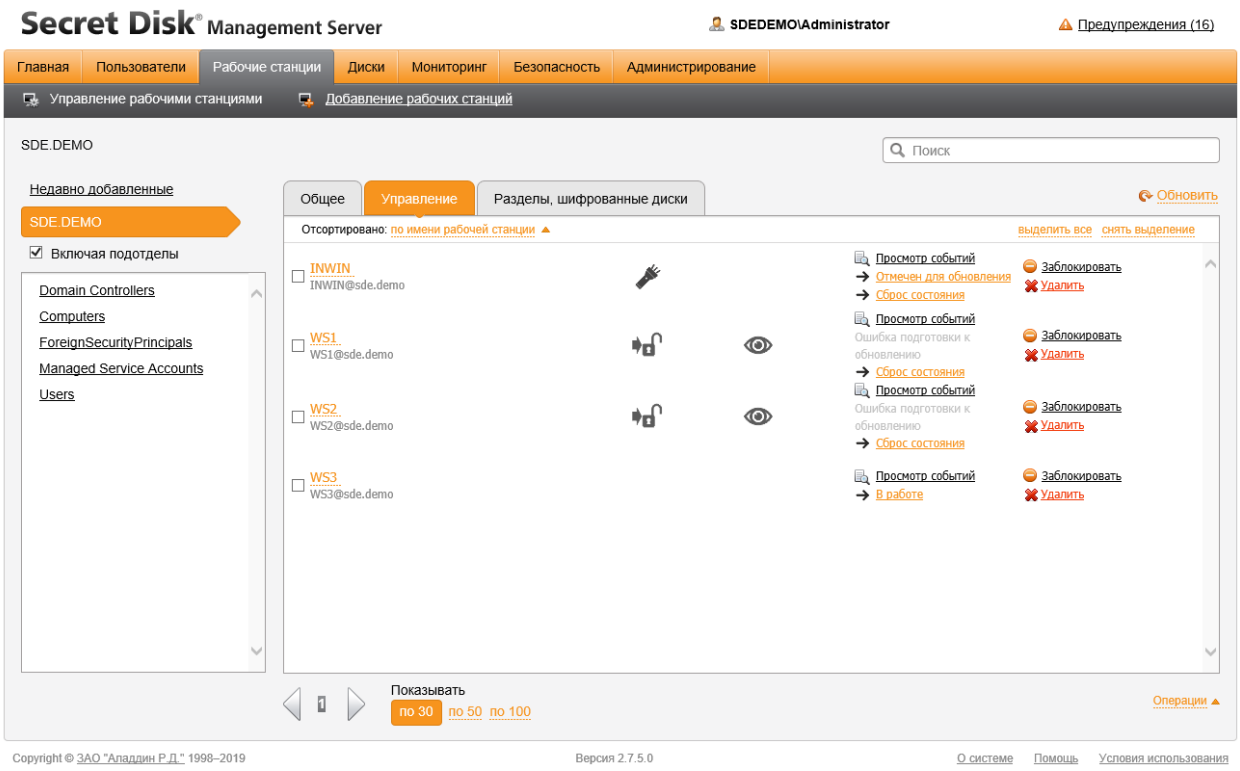
	Ошибка подготовки рабочей станции к обновлению. Ошибка расшифрования системного диска.
	Ошибка процесса защиты системного диска (зашифрования).

Для перевода рабочей станции в режим обновления выполните следующие действия:

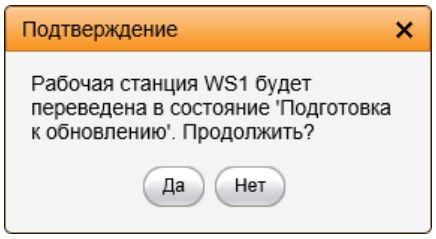
1. Отметьте рабочую станцию (рабочие станции) для начала процесса обновления.

> *Рабочую станцию можно отметить в **Журнале предупреждений** по ссылке Отметить для обновления или в меню **Рабочие станции** по ссылке В работе.*

Рабочая станция будет отмечена значком и иметь статус Отмечен для обновления.



2. Для перевода рабочей станции в следующее состояние (подготовка к обновлению) нажмите ссылку Отмечен для обновления. Подтвердите действие, нажав **Да**. Станция перейдёт в режим подготовки к обновлению и будет иметь соответствующее обозначение ( ).



> *Подготовка к обновлению означает, что началось расшифрование системного раздела рабочей станции. Обязательно дождитесь окончания процесса расшифрования!*

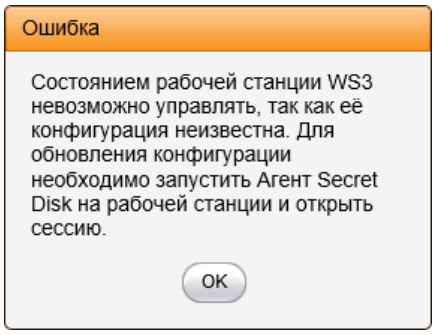
3. Если при расшифровании системного раздела возникнет ошибка, то в портале появится соответствующее уведомление .

> *При возникновении ошибки расшифрования системного диска обратитесь в техническую поддержку.*

4. После успешного завершения процесса расшифрования системного раздела знак поменяется на . Это значит, что системный раздел рабочей станции полностью расшифрован и можно начинать процесс обновления ОС.
5. Запустите процесс обновления ОС и дождитесь его окончания.
6. После успешного окончания процесса обновления ОС системный раздел можно заново защитить, нажав Готов к обновлению в окне **Управления рабочими станциями**. Начало процесса защиты сопровождается появлениям значка .

> *Дождитесь окончания процесса зашифрования системного раздела.*

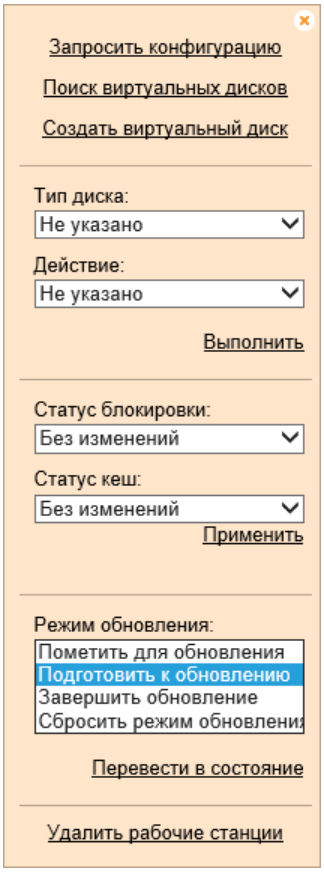
Если портал SDMS не получил (не обновил) конфигурацию рабочей станции, то появится следующее сообщение об ошибке:



Для корректной работы запустите Агент Secret Disk на рабочей станции пользователя и в портале SDMS запросите конфигурацию станции.

4.5.1 Групповые операции

Все настройки и переходы из состояния в состояние можно делать с помощью групповых операций. Для этого выберите флагом нужные станции → Операции → Выберите режим обновления → Перевести в состояние.

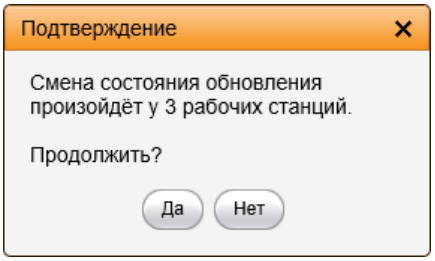


Если выделенные станции находятся в разных состояниях, то групповая операция будет доступна только для тех станций, которые нужно перевести в следующее состояние.

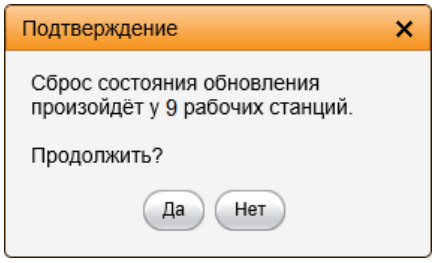
Т.е. если:

- 3 станции находятся в режиме Отмечен для обновления;
- 4 станции в режиме Подготовки к обновлению;
- 2 станции в Готов к обновлению.

Необходимо перевести станции в режим Подготовить к обновлению. В этот режим переведутся только 3 станции из 9 (из предыдущего состояния).



Если выделенные станции находятся в разных состояниях, то групповая операция **сброса** будет произведена для **всех** выделенных станций.



4.5.2 Сброс состояния

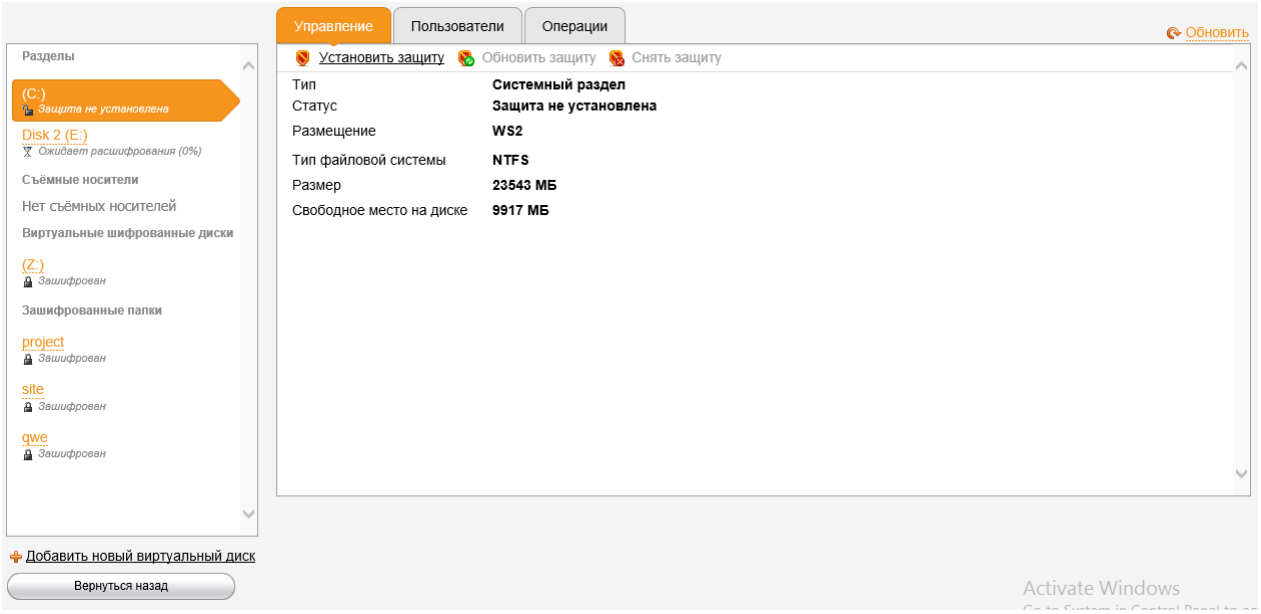
Сброс состояния – функция, при которой рабочая станция выходит из любого состояния и переводит ее в режим В работе.

Функция необходима для ручного перехода в начальное состояние рабочей станции для устранения возможных некорректных действий системы.

Например, при зашифровании системного диска была произведена некорректная тестовая перезагрузка рабочей станции пользователя.

1. При возникновении ошибки зашифрования системного диска ( ) зайдите во вкладку **Разделы, шифрованные диски** → выберите нужный диск **C:**.
2. Во вкладке **Рабочие станции → Управление** нажмите Установить защиту.

> *Произойдет автоматическое сбрасывание состояния обновления рабочей станции.*



> *В случае возникновения повторной ошибки защиты системного раздела рабочей станции рекомендуем обратиться в техническую поддержку.*

5. Авторские права, товарные знаки, ограничения

Ограничение ответственности

Информация, приведённая в данном документе, предназначена исключительно для ознакомления и не является исчерпывающей. Состав продуктов, компонент, их функции, характеристики, версии, доступность и пр. могут быть изменены ЗАО "Аладдин Р.Д." без предварительного уведомления.

ЗАО "Аладдин Р.Д." не гарантирует ни отсутствия ошибок в данном документе, ни того, что описанное программное обеспечение (ПО) не содержит дефектов, будет работать в произвольно выбранных условиях и при этом удовлетворять всем требованиям, которые могут быть к нему предъявлены.

ЗАО "Аладдин Р.Д." не гарантирует работоспособность нелегально полученного программного обеспечения. Нелегальное использование программного обеспечения и документации на него преследуется по закону.

Все указанные данные о характеристиках продуктов основаны на международных или российских стандартах и результатах тестирования, полученных в независимых тестовых или сертификационных лабораториях, либо на принятых в компании методиках. В данном документе ЗАО "Аладдин Р.Д." не предоставляет никаких ни явных, ни подразумеваемых гарантий.

ЗАО "Аладдин Р.Д." НЕ НЕСЁТ ОТВЕТСТВЕННОСТИ (КАК В СИЛУ ДОГОВОРА, ГРАЖДАНСКОГО ПРАВОНАРУШЕНИЯ, ВКЛЮЧАЯ ХАЛАТНОСТЬ, ТАК И В ЛЮБОЙ ИНОЙ ФОРМЕ) ПЕРЕД ВАМИ ИЛИ ЛЮБОЙ ТРЕТЬЕЙ СТОРОНОЙ ЗА ЛЮБЫЕ ПОТЕРИ ИЛИ УБЫТКИ (ВКЛЮЧАЯ КОСВЕННЫЕ, ФАКТИЧЕСКИЕ ИЛИ ПОБОЧНЫЕ УБЫТКИ), ВКЛЮЧАЯ БЕЗ ОГРАНИЧЕНИЙ ЛЮБЫЕ ПОТЕРИ ИЛИ УБЫТКИ ПРИБЫЛЬНОСТИ БИЗНЕСА, ПОТЕРЮ ДОХОДНОСТИ ИЛИ РЕПУТАЦИИ, УТРАЧЕННУЮ ИЛИ ИСКАЖЁННУЮ ИНФОРМАЦИЮ ИЛИ ДОКУМЕНТАЦИЮ ВСЛЕДСТВИЕ ИСПОЛЬЗОВАНИЯ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И/ИЛИ ЛЮБОГО КОМПОНЕНТА ОПИСАННОГО ПРОДУКТА, ДАЖЕ ЕСЛИ ЗАО "Аладдин Р.Д." БЫЛО ПИСЬМЕННО УВЕДОМЛЕНО О ВОЗМОЖНОСТИ ПОДОБНЫХ УБЫТКОВ.

Государственное регулирование и экспортный контроль

Описываемый в данном документе продукт (или продукты) может являться или содержать в себе средство криптографической защиты информации (СКЗИ), являющееся предметом экспортного контроля.

Вы соглашаетесь с тем, что продукт не будет поставляться, передаваться или экспортироваться в какую-либо страну, а также использоваться каким-либо противоречащим закону образом.

Вы гарантируете, что будете соблюдать накладываемые на экспорт и реэкспорт продукта ограничения.

Сведения, приведённые в данном документе, актуальны на дату его публикации.

5.1 Лицензионное соглашение

Пожалуйста, внимательно прочитайте данное лицензионное соглашение прежде, чем использовать содержимое данного комплекта и/или прежде, чем загружать или устанавливать программное обеспечение.

Все указания по использованию программного обеспечения, предоставляемые Закрытым акционерным обществом "Аладдин Р. Д." (или любым его дочерним предприятием – каждое из них упоминаемое как "компания"), подчиняются и будут подчиняться условиям, оговоренным в данном соглашении. Загружая данное программное обеспечение (как определено далее по тексту) и/или устанавливая данное программное обеспечение на Ваш компьютер и/или используя данное программное обеспечение иным способом, Вы принимаете данное соглашение и соглашаетесь с его условиями.

Если Вы не согласны с данным соглашением, не загружайте и/или не устанавливайте данное программное обеспечение и незамедлительно (не позднее 7 (семи) дней с даты ознакомления с настоящим текстом) верните этот продукт в ЗАО "Аладдин Р.Д.", удалите данное программное обеспечение и все его части со своего компьютера и не используйте его никоим образом.

Настоящее лицензионное соглашение (далее "Соглашение") является договором, заключенным между Вами (физическим или юридическим лицом) — конечным пользователем (далее "Пользователь") — и ЗАО "Аладдин Р.Д." (далее "Компания") относительно передачи неисключительного права на использование настоящего программного обеспечения, являющегося интеллектуальной собственностью Компании.

Права и собственность

ДАННОЕ СОГЛАШЕНИЕ НЕ ЯВЛЯЕТСЯ СОГЛАШЕНИЕМ О ПРОДАЖЕ. Программное обеспечение, включая все переработки, исправления, модификации, дополнения, обновления и/или усовершенствования к нему (далее по всему тексту и любой его части определяемое как Программное обеспечение или ПО), и связанная с ним документация предназначается НЕ ДЛЯ ПРОДАЖИ и является и остаётся исключительной собственностью Компании.

Все права на интеллектуальную собственность (включая, без ограничений, авторские права, коммерческую тайну, товарные знаки, и т.д.), подтверждённые или включённые в приложенные/взаимосвязанные/имеющие отношение к данному руководству, данные, содержащиеся в нём, а также все права на ПО являются и будут являться собственностью исключительно Компании.

Данное соглашение не передаёт Вам права на Программное обеспечение, а лишь предоставляет ограниченное право на использование, которое подлежит отмене согласно условиям данного Соглашения. Ничто в данном Соглашении не подтверждает отказ Компании от прав на интеллектуальную собственность по какому бы то ни было законодательству.

Лицензия

Компания настоящим предоставляет Вам, а Вы получаете индивидуальное, неисключительное и отзываемое ограниченное право на использование данного ПО только в форме исполняемого кода, как описано в прилагаемой к ПО технической/эксплуатационной документации, и только в соответствии с условиями данного **Соглашения:**

Вы можете установить ПО и использовать его на компьютерах, расположенных в пределах Вашего предприятия, как описано в соответствующей технической/эксплуатационной документации ПО и в настоящем соглашении.

Вы можете добавить/присоединить Программное обеспечение к программам для мобильных устройств с единственной целью, описанной в данном Соглашении. Принимая условия настоящего соглашения, Вы соглашаетесь:

- не использовать, не модифицировать и не выдавать сублицензии на данное Программное обеспечение и любое другое ПО Компании, за исключением явных разрешений в данном Соглашении;

- не модифицировать, не демонтировать, не декомпилировать, не реконструировать, не видоизменять и не расширять данное Программное обеспечение и не пытаться раскрыть (получить) исходные коды данного Программного обеспечения;

- не помещать данное Программное обеспечение на сервер с возможностью доступа к нему третьих лиц через открытую сеть;

- не использовать какие бы то ни было резервные или архивные копии данного Программного обеспечения (или позволять кому-либо ещё использовать такие копии) с любой иной целью, кроме замены его оригинального экземпляра в случае его разрушения или наличия дефектов.

Требования к использованию

Программное обеспечение должно использоваться и обслуживаться строго в соответствии с описаниями и инструкциями Компании, приведёнными в данном и других документах Компании, в том числе на портале онлайн документации для разработчиков Компании (http://developer.aladdin-rd.ru/).

Использование ПО

Пользователь вправе:

- воспроизводить ПО путём записи его в память электронно-вычислительных машин Пользователя, ограниченное правом инсталляции, копирования и запуска программ для ЭВМ;

- встраивать ПО любым способом в продукты и решения Пользователя;

- распространять ПО любым способом исключительно в составе продуктов и решений Пользователя.

При использовании и распространении ПО Пользователь обязан руководствоваться действующим законодательством Российской Федерации и международным законодательством, учитывая ограничения и дополнительные требования, которые могут возникать в связи с экспортом шифровальных (криптографических) средств с территории Российской Федерации и импортом таких средств в другие страны. В частности, ограничения и дополнительные требования могут возникать при распространении ПО через магазины приложений, содержащие различные приложения для мобильных устройств.

Условия использования, изложенные в настоящем соглашении, действуют в отношении всего содержимого ПО, в частности в отношении:

- дизайна (графики, расположения элементов оформления и т.п.);

- всех иных элементов, в том числе изображений, фонограмм, текстов.

Получаемые Пользователем неисключительные имущественные права не включают права на передачу третьим лицам каких-либо прав на встраивание, воспроизведение, распространение и использование программ для ЭВМ не в составе продуктов и решений Пользователя.

Компания сохраняет за собой все исключительные права на ПО и входящие в него компоненты, включая права на предоставление неисключительных и исключительных прав третьим лицам.

Пользователь вправе осуществлять использование ПО в пределах, предусмотренных настоящим Соглашением, исключительно на территории Российской Федерации.

Обслуживание и поддержка

Компания не несёт обязательств по предоставлению поддержки, обслуживания, модификации или выходу новых релизов ПО.

Ограниченная гарантия

Компания гарантирует, что программное обеспечение с момента приобретения его Вами в течение 12 (двенадцати) месяцев будет функционировать в полном соответствии с его технической/эксплуатационной документацией, при условии, что ПО будет использоваться на компьютерном аппаратном обеспечении и с операционной системой, для которой оно было разработано.

Отказ от гарантии

Компания не гарантирует, что программное обеспечение будет соответствовать Вашим желаниям и требованиям, или что его работа будет бесперебойной или безошибочной. В объёме, предусмотренном законодательством РФ, компания открыто отказывается от всех гарантий, не оговоренных здесь, от всех иных подразумеваемых гарантий. Ни один из дилеров, дистрибьюторов, продавцов, агентов

или сотрудников компании не уполномочен производить модификации, расширения или дополнения к данной гарантии.

Если Вы произвели какие-либо модификации ПО или любой из его частей во время гарантийного периода, ПО подверглось повреждению, неосторожному или неправильному обращению, если Вы нарушили любое из условий настоящего Соглашения, то гарантия, упомянутая выше в разделе 5, будет немедленно прекращена.

Гарантия недействительна, если ПО используется в сочетании с иным аппаратным и/или программным обеспечением, отличным от описанных в технической/эксплуатационной документации, или используется на компьютере с любым установленным нелицензионным программным обеспечением.

Ограничение возмещения

В случае нарушения гарантии, оговоренной выше, Компания может по собственному усмотрению:

- заменить ПО, если это не противоречит вышеупомянутому ограничению гарантии;

- возместить стоимость, выплаченную Вами за ПО.

Гарантийные требования должны быть выставлены в письменном виде в течение гарантийного периода, но не позднее 7 (семи) дней с момента обнаружения дефекта, и содержать в себе подтверждения, удовлетворяющие Компанию. Всё ПО (все экземпляры, имеющиеся у Вас) должно быть возвращено Компании и отправлено возвращающей стороной с оплаченной стоимостью перевозки и, при необходимости, страховки. Экземпляры ПО должны быть отправлены с копией платёжных документов и накладных.

Исключение косвенных убытков

Стороны признают, что Программное обеспечение не может быть полностью лишено ошибок. Компания не несёт ответственности (как в силу договора, гражданского правонарушения, включая халатность, так и в любой иной форме) перед Вами или любой третьей стороной за любые потери или убытки (включая косвенные, фактические, побочные или потенциальные убытки), включая, без ограничений, любые потери или убытки прибыльности бизнеса, потерю доходности или репутации, утраченную или искажённую информацию или документацию вследствие какого-либо использования данного программного обеспечения и/или любой компоненты данного по, даже если компания письменно уведомлена о возможности подобных убытков.

Ограничение ответственности

В случае если, несмотря на условия данного соглашения, компания признана ответственной за убытки на основании каких-либо дефектов или несоответствия программного обеспечения Вашим ожиданиям, полная ответственность за каждый экземпляр дефектного программного обеспечения не будет превышать суммы, выплаченной вами ЗАО "Аладдин Р.Д." за это ПО.

Прекращение действия соглашения

В случае невыполнения Вами условий данного Соглашения действие Вашей лицензии и настоящего Соглашения будет прекращено.

После прекращения действия данного Лицензионного соглашения:

- лицензия, предоставленная Вам данным Соглашением, прекращает своё действие, и Вы после её прекращения не сможете продолжать дальнейшее использование данного Программного обеспечения и других лицензионных Продуктов;

- вы незамедлительно вернёте в Компанию все экземпляры ПО и все копии такового и/или сотрёте/удалите любую информацию, содержащуюся в электронном виде.

Применимое законодательство

Данное Соглашение должно быть истолковано и определено в соответствии с законодательством Российской Федерации (за исключением конфликта применения правовых норм), и только российский суд уполномочен осуществлять правосудие в любых конфликтах и спорах, вытекающих из данного Соглашения. Невозможность для любой из сторон воспользоваться любым из прав, предоставленных ей по данному Соглашению, или принять меры против другой стороны в случае любого нарушения своих обязательств по Соглашению не должно рассматриваться как отказ этой стороны от последующего понуждения к признанию своих прав или совершению последующих действий в случае дальнейших нарушений.

Государственное регулирование и экспортный контроль

Вы соглашаетесь с тем, что ПО не будет Вами поставляться, передаваться или экспортироваться в какую-либо страну, а также использоваться каким-либо противоречащим закону и условиям настоящего соглашения образом. ПО является предметом дополнительного экспортного контроля, относящегося к Вам или Вашей юрисдикции. Вы гарантируете, что будете соблюдать накладываемые ограничения на экспорт и реэкспорт ПО.

Разное

Настоящее Соглашение представляет собой полное соглашение, относящееся к данной лицензии, и может быть изменено только посредством письменного соглашения, подписанного обеими сторонами. Если выполнение какого-либо условия настоящего Соглашения представляется невозможным, такое условие будет скорректировано только в пределах, обеспечивающих возможность выполнения данного условия.

Я ПРОЧИТАЛ И ПОНЯЛ НАСТОЯЩЕЕ ЛИЦЕНЗИОННОЕ СОГЛАШЕНИЕ И СОГЛАСЕН ВЫПОЛНЯТЬ ВСЕ ЕГО УСЛОВИЯ. Я ПРИНИМАЮ ДАННОЕ ЛИЦЕНЗИОННОЕ СОГЛАШЕНИЕ ЦЕЛИКОМ. ЕСЛИ Я НЕ ПРИНИМАЮ ЭТО ЛИЦЕНЗИОННОЕ СОГЛАШЕНИЕ ИЛИ ХОТЯ БЫ ОДИН ИЗ ЕГО ПУНКТОВ, ТО ДАННОЕ ЛИЦЕНЗИОННОЕ СОГЛАШЕНИЕ НЕ ВСТУПАЕТ В СИЛУ, И Я ОБЯЗУЮСЬ НЕ УСТАНАВЛИВАТЬ И НЕ ИСПОЛЬЗОВАТЬ ДАННОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ.

6. Контакты

6.1 Офис (общие вопросы)

Адрес: 129226, Москва, ул. Докукина, д. 16, стр. 1, 7 этаж, компания "Аладдин Р.Д."

Телефоны: +7 (495) 223-00-01 (многоканальный), +7 (495) 988-46-40

Факс: +7 (495) 646-08-82

E-mail: aladdin@aladdin-rd.ru (общий)

Web: https://www.aladdin-rd.ru

Время работы: ежедневно с 10:00 до 19:00, кроме выходных и праздничных дней.

6.2 Техподдержка

Служба техподдержки принимает запросы только в письменном виде через веб-сайт: www.aladdin-rd.ru/support/index.php.

7. Регистрация изменений

Версия	Изменения
1.0 draft	В работе
0.9 draft	Описаны разделы 2-3
0.3 draft	Создание документа
2.0	Добавлен раздел 4. Добавлено полное описание процесса обновления. Вставлены названия таблиц и рисунков. Обновлены скриншоты.

5) 223-00-01 Email: aladdin@aladdin-rd.ru Web: www.aladdin-

Коротко о компании

Компания "Аладдин Р.Д." основана в апреле 1995 года и является российским разработчиком (вендором) средств защиты информации.

Компания является признанным экспертом и лидером российского рынка средств двухфакторной аутентификации пользователей, электронной подписи и защиты данных.

Основные направления

- Обеспечение безопасного доступа к информационным ресурсам предприятия, веб-порталам и облачным сервисам (строгая двух- и трёхфакторная аутентификация).
- Электронная подпись (ЭП с неизвлекаемым закрытым ключом, формируемая в защищённом чипе), PKI.
- Защита персональных данных, данных на дисках компьютеров, серверов, баз данных.
- Все основные продукты имеют необходимые сертификаты ФСТЭК, ФСБ и Министерства обороны (включая работу с гостайной до уровня секретности СС).

Лицензии

- компания имеет все необходимые лицензии ФСТЭК России, ФСБ России и Министерства обороны России для проектирования, производства и поддержки СЗИ и СКЗИ, включая работу с гостайной и производство продукции в рамках гособоронзаказа.
- Система менеджмента качества продукции в компании с 2012 г. соответствует стандарту ГОСТ ISO 9001-2011 и имеет соответствующие сертификаты.
- Система проектирования, разработки, производства и поддержки продукции соответствует требованиям российского военного стандарта ГОСТ РВ 15.002-2012, необходимого для участия в реализации гособоронзаказа.